

Dr.WEB®

Antivirus pour Linux

Defend what you create

Mode d'emploi

Dr.Web® Antivirus pour Linux
Version 10.1.0
Mode d'emploi
10.04.2015

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Consultez le site web officiel pour en savoir plus sur les bureaux régionaux ou internationaux.

Doctor Web

Doctor Web développe et distribue les solutions de sécurité de l’information Dr.Web® qui fournissent une protection efficace contre les logiciels malveillants et le spam.
Les clients de Doctor Web sont des utilisateurs particuliers dans le monde entier, ainsi que des institutions gouvernementales, des petites entreprises et des entreprises nationales.
Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des malwares et leur conformité aux standards de sécurité de l’information internationaux. Les certificats d’Etat et les prix attribués aux solutions Dr.Web ainsi que l’utilisation de nos produits dans le monde entier sont les meilleurs témoins de la confiance qui leur est accordée.

Nous remercions tous nos clients pour leur soutien et leur fidélité aux produits Dr.Web !



Contenu





Charte du document

La charte et les symboles suivants sont utilisés dans ce manuel :

Charte	Description
Gras	Noms des boutons et autres éléments de l'interface graphique utilisateur (GUI), ainsi que les contributions de l'utilisateur, qui doivent être entrés exactement comme indiqué dans le guide.
Vert et gras	Noms des produits et composants de **Dr.Web**.
Vert et souligné	Hyperliens vers les sujets et pages web.
`Monospace`	Exemples de code, entrées dans la ligne de commande et sortie des applications. Dans le Manuel, les commandes à saisir par le clavier dans la ligne de commande du système d'exploitation (dans le terminal ou l'émulateur de terminal) sont introduites par le caractère `$` ou `#` qui indique les privilèges requis pour l'exécution de cette commande. Pour les systèmes UNIX : `$` – signifie que l'exécution de la commande requiert les privilèges ordinaires de l'utilisateur `#` – signifie que l'exécution de la commande requiert les privilèges de super-utilisateur (d'habitude – `root`). Pour élever les privilèges,on peut utiliser la commande **`su`** ou la commande **`sudo`**.
Italique	Espaces réservés aux informations devant être renseignées par l'utilisateur. Pour l'entrée dans la ligne de commande, cela indique les valeurs d'un paramètre. En plus, cela peut indiquer un terme dans une définition.
LETTRES MAJUSCULES	Noms des touches et des séquences de touches.
Signe plus ('+')	Indique une combinaison de touches. Par exemple, ALT+F1 signifie de maintenir la touche ALT tout en pressant la touche F1.
	Une alerte sur des erreurs éventuelles ou un autre événement important.

Introduction

Merci d’avoir acheté **Dr.Web® Antivirus pour Linux** (ci-après **Dr.Web pour Linux**). Il fournit une protection fiable contre différents types de menaces informatiques en utilisant les technologies les plus avancées de détection et de neutralisation des virus.

Ce manuel est destiné à aider les utilisateurs dont les ordinatuers tournent sous les OS de la famille **GNU/Linux** (**Linux** ci-après) installer et utiliser **Dr.Web pour Linux** 10.1.0.

Si **Dr.Web pour Linux** de la version antérieure est déjà installé sur votre ordinateur et que vous souhaitez mettre à niveau **l’Anti-virus** vers la version 10.1.0, suivez les étapes de la procédure de mise à niveau.



A propos de ce produit

Dr.Web pour Linux est une solution antivirus destinée à protéger les ordinateurs tournant sous les OS de la famille **GNU/Linux** contre les virus et autres types de menaces.

Les principaux composants du logiciel (le moteur antivirus **Dr.Web Virus-Finding Engine** et les bases virales de **Dr.Web**) ne sont pas uniquement très efficaces et économes en ressources, mais également multi plateforme, ce qui permet aux experts de **Dr.Web** de créer des solutions antivirus fiables pour les systèmes d'exploitation portables et serveurs les plus répandues (pour les OS de la famille **UNIX**, y compris **Mac OS X** et **GNU/Linux** ; **Windows**), ainsi que pour les appareils mobiles tournant sous **iOS** et **Android**.

Les composants de **Dr.Web pour Linux** sont constamment mis à jour et les bases virales s'enrichissent régulièrement de nouvelles signatures pour garantir une protection toujours à jour. De plus, des méthodes d'analyse heuristique sont utilisées pour fournir une protection supplémentaire contre les virus inconnus et la connexion au service **Dr.Web Cloud** collectant l'information la plus actuelle sur les menaces.

Fonctionnalités principales

Dr.Web pour Linux fournit les fonctions suivantes :

1. **Détection et neutralisation** des programmes malveillants (par exemple, des virus, y compris ceux qui infectent les boîtes de réception et les enregistrements d'amorçage, les Trojans, les vers de mail) et des logiciels non sollicités (par exemple, les adwares, canulars et dialers).

   Dr.Web pour Linux utilise plusieurs méthodes de détection des logiciels malveillants simultanément :

   * *L'analyse par signature* qui permet la détection des menaces connues
   * *L'analyse heuristique* qui permet la détection des menaces qui ne sont pas référencées dans la base de données virales
   * *Connexion au service* **Dr.Web Cloud**, qui collecte l'information la plus actuelle sur les menaces, envoyée par les produits antivirus différents **Dr.Web**

   Notez que *l'analyseur heuristique* peut augmenter les faux positif. Comme un objet peut être considéré à tort comme malveillant, toutes les menaces détectées par *l'analyseur heuristique* sont traitées comme suspectes. Ainsi, il est recommandé de ne pas supprimer ces menaces mais de les déplacer en quarantaine et de les envoyer au **Laboratoire Viral de Doctor Web** pour être analysées. Pour en savoir plus sur les méthodes de neutralisation des menaces, veuillez vous référer à Combattre les menaces informatiques (Annexe B).

   Les objets système sont scannés sur demande de l'utilisateur ou automatiquement, selon la planification. L'utilisateur peut lancer un scan de tous les objets du système de fichiers (les fichiers et les enregistrements d'amorçage) accessibles ou bien sélectionner le scan personnalisé pour que seuls les fichiers, répertoires et enregistrements d'amorçage spécifiés soient scannés. Il est également possible de lancer uniquement un scan des fichiers exécutables binaires contenant le code des processus en cours d'exécution. Si une menace est détectée dans ce cas de figure, l'objet malveillant est neutralisé et le processus actif est stoppé.

2. **Surveiller l'accès aux fichiers de données et les tentative de lancer des exécutables**. Cette fonctionnalité permet la détection et la neutralisation des malwares juste au moment d'une tentative d'infection.

3. **Gérer l'accès à Internet.**Cette fonctionnalité permet de contrôler les tentatives d'accès aux serveurs Internet et, si nécessaire, de bloquer les sites web ajoutés aux listes noires. Les fichiers téléchargés sur Internet sont contrôlés « à la volée ». Pour restreindre l'accès aux sites web non désirés, **Dr.Web pour Linux** utilise les thèmes des listes noires (fournies avec **Dr.Web pour**

Linux et mises à jour automatiquement) et les listes noires et blanches utilisateur (configurées par l'utilisateur) Une connexion au service **Dr.Web Cloud** est également effectuée pour vérifier, si la ressource web à laquelle l'utilisateur veut accéder n'est pas marquée comme malveillante par les autres produits de **Dr.Web**.



La version actuelle du produit ne peut pas surveiller l'accès Internet via les protocoles sécurisés, tels que HTTPS.

4. **Isolation fiable des objets infectés ou suspects.** Ces objets sont déplacés dans un dossier de stockage spécial, la quarantaine, pour prévenir tout endommagement du système. Lors du déplacement en Quarantaine, les objets sont renommés selon des règles spécifiques et, si nécessaire, ils peuvent être restaurés dans leur emplacement d'origine sur simple requête de l'utilisateur.
5. **Mise à jour automatique** des bases virales de **Dr.Web** et du moteur antivirus pour permettre à **Dr.Web pour Linux** d'utiliser les données les plus récentes à propos des logiciels malveillants connus.
6. **Fonctionnement en mode Protection centralisée** (s'il y a une connexion au serveur de protection centralisée, comme avec **Dr.Web Enterprise Server** ou dans le service **Dr.Web AV-Desk**). Ce mode permet d'implémenter une politique de sécurité unifiée sur les ordinateurs du réseau protégé. Cela peut être un réseau corporate, un réseau privé (VPN), ou le réseau d'un fournisseur de services (par exemple, un FAI).



Vu que l'utilisation de l'information stockée sur le service **Dr.Web Cloud**, requiert la transmission de données concernant l'activité de l'utilisateur (notamment – la transmission des adresses de sites web à vérifier), la connexion à **Dr.Web Cloud** est effectuée seulement après l'autorisation de l'utilisateur. Si cela est nécessaire, vous pouvez interdire l'utilisation de **Dr.Web Cloud** à tout moment.

Structure du Logiciel

Dr.Web pour Linux contient les composants suivants:

Composants	Description
Scanner	Scan des objets du système de fichiers (fichiers, répertoires, enregistrements d'amorçage) contre les menaces. Le scan peut être lancé sur demande de l'utilisateur ou sur planification. L'utilisateur peut lancer un scan depuis les modes graphique et ligne de commande.
SpIDer Guard moniteur du système de fichiers	Il fonctionne en mode résident et surveille les opérations du système de fichiers (comme créer, ouvrir, et fermer un fichier). Il envoie les requêtes du **Scanner** pour vérifier les contenus des nouveaux fichiers ou des fichiers modifiés et les contenus des exécutables lorsqu'il y a une tentative de les lancer.
SpIDer Gate Moniteur d'accès Internet	Composant fonctionnant en mode résident et contrôlant toutes les tentatives d'accès aux ressources web. Il vérifie si les URL demandées se trouvent dans les listes noires et, si c'est le cas, bloque l'accès à ces ressources. Il envoie les requêtes du **Scanner** pour scanner les fichiers téléchargés d'Internet (depuis les serveurs web autorisés). En plus, si l'utilisateur l'autorise, il envoie les URL requises pour les vérifier au service **Dr.Web Cloud.**
Moteur antivirus	Composant central de la protection antivirus utilisé par le **Scanner** pour la recherche et la détection des menaces ainsi que pour l'analyse du comportement des objets suspects.
Bases de données virales	Bases de données mises à jour automatiquement utilisées par le moteur antivirus et contenant des informations pour la détection et la neutralisation des menaces connues.
Updater	Il télécharge les mises à jour des bases de données virales et du moteur antivirus sur



Composants	Description
	les serveurs de mise à jour de **Doctor Web** automatiquement, en fonction de la planification ou sur demande de l'utilisateur.
Gestionnaire de licences	Il aide les utilisateurs à gérer leurs licences et effectue les actions suivantes : activer une licence et une version démo, fournir de l'information sur la licence en cours, renouveler la licence, ainsi qu'installer ou supprimer un fichier clé de licence.

A part les composants décrits dans le tableau, **Dr.Web pour Linux** inclut des composants de service qui opèrent en tâche de fond et ne requièrent pas l'intervention de l'utilisateur.



SpIDer Guard, le moniteur du système de fichiers, peut opérer dans un des modes suivants:

* `FANOTIFY` – en utilisant l'interface de gestion **`fanotify`** (tous les OS basés sur **GNU/Linux**-ne supportent pas **`fanotify`**)
* `LKM` – en utilisant le module noyau chargeable **Linux** (compatible avec n'importe quel OS basé sur **GNU/Linux**avec un noyau `2.6.x` et supérieur)

Par défaut, le moniteur du système de fichiers choisit automatiquement le mode opératoire approprié selon l'environnement. Si **SpIDer Guard** ne peut pas démarrer, créez et installez un module noyau chargeable en utilisant les codes source fournis.

Répertoires de la quarantaine

Le répertoire de la quarantaine sert à isoler les fichiers qui constituent une menace pour la sécurité du système et ne peuvent pas être traités. Ces menaces sont inconnues de **Dr.Web pour Linux** (c'est-à-dire qu'un virus est détecté par *l'analyseur heuristique* mais que la signature du virus et la méthode de traitement ne sont pas présentes dans les bases virales) ou elles ont provoqué une erreur durant le scan. De plus, un fichier peut être placé en quarantaine sur demande de l'utilisateur si il a sélectionné cette action dans la liste des menaces détectées ou s'il a spécifié cette action dans le **Scanner** ou dans les paramètres de **SpIDer Guard** comme la réaction à adopter face à une menace de ce type.

Lorsqu'un fichier est placé en quarantaine, il est renommé selon des règles spécifiques. Le renommage des fichiers isolés empêche les utilisateurs et les applications d'accéder à ces fichiers s'ils outrepassent les outils de gestion de la quarantaine implémentés dans **Dr.Web pour Linux.**

Les répertoires de la quarantaine sont situés dans

* **Le répertoire racine Utilisateur** (si plusieurs comptes utilisateurs existent sur l'ordinateur, un répertoire de quarantaine séparé peut être créé pour chaque utilisateur)
* **Le répertoire racine** de chaque volume logique du système de fichiers

Les répertoires de quarantaine de **Dr.Web** sont toujours nommés sous le format **`.com.drweb.quarantine`** et ne sont pas créés tant que l'action **`(Isolate)`** en **`Quarantaine`** est appliquée. Ainsi, seul un répertoire requis pour l'isolation d'un objet concret est créé. Lors de la sélection d'un répertoire, le nom du propriétaire du fichier est utilisé : la recherche est effectuée vers le haut depuis l'emplacement de l'objet malveillant et si le répertoire racine du propriétaire est atteint, le dossier de stockage de quarantaine créé est utilisé. Sinon, le fichier est isolé dans la quarantaine créée dans le répertoire racine du volume (qui n'est pas toujours le même que le répertoire racine du système de fichiers). Ainsi, n'importe quel fichier déplacé en quarantaine réside toujours sur le volume qui permet un fonctionnement correct de la quarantaine au cas où plusieurs supports de stockage amovibles et d'autres volumes sont créés à différents emplacements dans le système.

Les utilisateurs peuvent gérer les objets en quarantaine soit en mode graphique soit avec la ligne de commande. Chaque action est appliquée à la quarantaine consolidée ; c'est-à-dire que les modifications affectent tous les répertoires de la quarantaine disponibles au moment de ces modifications. Du point de vue de l'utilisateur, le répertoire de quarantaine situé dans le répertoire source de l'utilisateur est considéré comme la *Quarantaine Utilisateur* et les autres répertoires sont

considérés comme la *Quarantaine Système*.



Travailler avec des objets de quarantaine est autorisé uniquement si aucune licence active n'est trouvée. Cependant, les objets isolés ne peuvent pas être traités dans ce cas.

Permissions et privilèges des fichiers

Pour scanner les objets du système de fichiers et neutraliser les menaces, **Dr.Web pour Linux** (ou plutôt l'utilisateur sous lequel **Dr.Web pour Linux** fonctionne) requiert les permissions suivantes:

Action	Permissions requises
Liste de toutes les menaces détectées	Illimité. Aucune permission spécifique n'est requise.
Liste des contenus des archives (uniquement les éléments malveillants ou corrompus)	Illimité. Aucune permission spécifique n'est requise.
Déplacer en quarantaine	Illimité. L'utilisateur peut placer en quarantaine tous les fichiers infectés quelles que soient les permissions de lecture ou d'écriture les concernant.
Supprimer une menace	L'utilisateur doit avoir la permission d'écrire sur le fichier supprimé.
Réparer	Illimité. Les permissions et la propriété d'un fichier réparé demeurent les mêmes. Si la suppression est appliquée au fichier durant le traitement, il est supprimé du système quelles que soient les permissions de l'utilisateur le concernant.
Restaurer un fichier de la quarantaine	L'utilisateur doit avoir les permissions de lecture du fichier et d'écriture dans le répertoire restauré.
Supprimer un fichier de la quarantaine	L'utilisateur doit avoir les permissions sur le fichier qui a été déplacé en quarantaine.

Pour élever temporairement les privilèges de **Dr.Web pour Linux** en mode graphique, cliquez sur le bouton correspondant dans la fenêtre de **Dr.Web pour Linux**. Pour activer le fonctionnement de **Dr.Web pour Linux** en mode graphique ou l'outil de gestion de la ligne de commande avec les privilèges super utilisateur, vous pouvez utiliser la commande `su`, qui permet de modifier l'utilisateur, ou la commande `sudo`, qui permet d'exécuter une commande en tant qu'autre utilisateur.



Notez que le **Scanner** ne peut pas vérifier les fichiers dont la taille dépasse 4Go (en cas de tentative de scanner de tels fichiers, un message d'erreur s'affiche : « Fichier trop volumineux ».

Modes de fonctionnement

Dr.Web pour Linux peut fonctionner en mode stand-alone ou bien comme partie d'un réseau antivirus géré par un serveur de protection centralisée. Le fonctionnement en mode Protection centralisée ne requiert pas l'installation d'un logiciel supplémentaire ou bien la réinstallation ou la suppression de **Dr.Web pour Linux**.

- **En mode Stand-alone**, l'ordinateur protégé n'est pas connecté à un réseau antivirus et son fonctionnement est géré localement. Dans ce mode, les fichiers clés de licence et de configuration se trouvent sur les disques locaux et **Dr.Web pour Linux** est totalement contrôlé depuis l'ordinateur protégé. Mises à jour des bases virales sont reçues des serveurs de mise à jour de **Doctor Web**.
- **En mode Protection centralisée**, la protection de l'ordinateur est gérée par le serveur de protection centralisée. Dans ce mode, certaines fonctionnalités et paramètres de **Dr.Web pour Linux** peuvent être configurés en accord avec la politique générale (corporate) de protection



antivirus mise en œuvre dans le réseau antivirus. Le fichier clé de licence utilisé pour le mode Protection centralisée est reçu du serveur de protection centralisée Le fichier clé conservé sur un ordinateur local, s'il en existe un, n'est pas utilisé. Les statistiques sur les événements viraux sont envoyées au serveur de protection centralisée Les mises à jour des bases virales sont également reçues du serveur de protection centralisée.

- **En mode Mobile**, **Dr.Web pour Linux** reçoit les mises à jour des serveurs de mise à jour de **Doctor Web**, mais le fonctionnement de **Dr.Web pour Linux** est géré avec les paramètres locaux. Le fichier clé utilisé est reçu du serveur de protection centralisée.

Lorsque **Dr.Web pour Linux** fonctionne en mode Protection centralisée ou Mobile, les options suivantes sont bloquées :

1. Suppression d'un fichier clé de licence dans le **Gestionnaire de licences**
2. Démarrage manuel d'un processus de mise à jour et configuration des paramètres de mise à jour
3. Configuration des paramètres de scan du système de fichiers

La configuration des paramètres de **SpIDer Guard** comme l'option permettant d'activer ou désactiver les vérifications de **SpIDer Guard** est autorisée en fonction des permissions spécifiées sur le serveur.



Notez que si le lancement du scan sur demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, la page de lancement du scan et bouton **Scanner** de la fenêtre de **Dr.Web pour Linux** sera désactivée. De plus, dans ce cas, le **Scanner** ne lancera pas des scans planifiés.

Structure logique du réseau antivirus

Les solutions **Doctor Web** pour la protection centralisée utilisent un modèle client-serveur (voir l'image ci-dessous).

Les postes de travail et les serveurs sont protégés par des *composants antivirus locaux* (ci-après, **Dr.Web pour Linux**) qu'on leur a installés et qui fournissent une protection antivirus des ordinateurs distants et permettent la connexion entre les postes de travail et le serveur de protection centralisée.

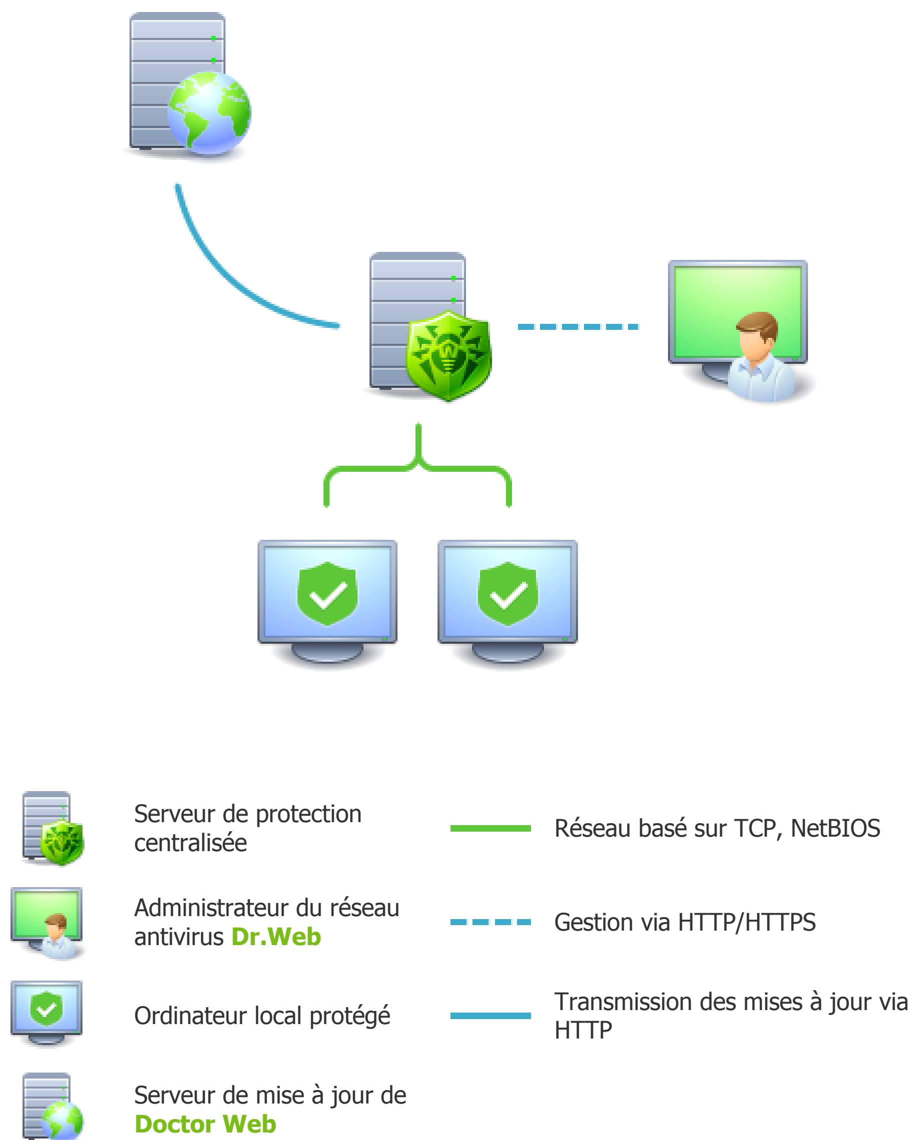


Image 1. Structure logique du réseau antivirus

Les ordinateurs locaux sont mis à jour et configurés depuis le *serveur de protection centralisée*. Le flux d'instructions, données et statistiques dans le réseau antivirus passe également par le serveur de protection centralisée. Le volume de trafic entre les ordinateurs protégés et le serveur central peut être assez important, c'est pourquoi nos solutions fournissent des options de compression de trafic. Pour prévenir la fuite de données sensible ou la substitution de logiciels téléchargés sur des ordinateurs protégés, le chiffrement est également supporté.

Toutes les mises à jour nécessaires sont téléchargées sur le serveur de protection centralisée depuis les serveurs de mise à jour de **Doctor Web**.

Les composants antivirus locaux sont configurés et gérés depuis le serveur de protection centralisée d'après les commandes des administrateurs du réseau antivirus. Les administrateurs gèrent les serveurs de protection centralisée et la topologie du réseau antivirus (par exemple, valider les connexions des ordinateurs distants au serveur de protection centralisée) et configurent les composants antivirus locaux si nécessaire.





Les composants antivirus locaux ne sont pas compatibles avec les produits antivirus d'autres éditeurs ou des produits de **Dr.Web** si cette dernière ne supporte pas un fonctionnement en mode Protection centralisée (par exemple, la version 5.0 de **Dr.Web pour Linux**). L'installation de deux produits antivirus sur le même ordinateur peut provoquer le crash du système et une importante perte de données.

Connexion au réseau antivirus

Dr.Web pour Linux peut être connecté à un réseau antivirus d'une des façons suivantes :

- Durant l'activation de **Dr.Web pour Linux**– dans le **Gestionnaire de licences**
- A l'onglet **Mode** de la fenêtre des paramètres dans l'interface graphique de **Dr.Web pour Linux**
- Utiliser la commande `esconnect` de l'outil de gestion de la ligne de commande – **`drweb-ctl`**

Se déconnecter du Réseau Antivirus

Dr.Web pour Linux peut être déconnecté du réseau antivirus d'une des façons suivantes :

- A l'onglet **Mode** de la fenêtre des paramètres dans l'interface graphique de **Dr.Web pour Linux**
- Utiliser la commande `esconnect` de l'outil de gestion de la ligne de commande – – **`drweb-ctl`**

Tester le fonctionnement de l'antivirus

Le test `EICAR` *(European Institute for Computer Anti-Virus Research)* permet de tester les performances des programmes antivirus utilisant la méthode de détection par signatures. Ce test a été spécialement conçu pour que les utilisateurs puissent tester les capacités de détection des outils antivirus nouvellement installés sans compromettre la sécurité de leur ordinateur.

Bien que `EICAR` ne soit pas un virus, il est traité par la plupart des antivirus comme tel. Au moment de la détection de ce "virus", les produits antivirus **Dr.Web** affichent l'information suivante : **`EICAR Test File (Not a Virus!)`**. D'autres outils antivirus alertent les utilisateurs de la même façon. Le fichier test `EICAR` est un fichier COM de 68 octets pour Windows MS DOS/MS qui indique la ligne suivante sur la console au moment de son exécution :

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Le test `EICAR` contient la chaîne de caractères suivante seulement :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Pour créer votre propre fichier test avec le « virus », vous devez créer un nouveau fichier contenant la ligne susmentionnée.

Si **Dr.Web pour Linux** fonctionne correctement, le fichier test `EICAR` est détecté durant le scan du système de fichiers quel que soit le mode de scan, et l'utilisateur est prévenu qu'une menace a été détectée : **`EICAR Test File (Not a Virus!)`**.



Pré-requis système

Vous pouvez utiliser **Dr.Web pour Linux** sur un ordinateur répondant aux pré-requis suivants :

Description	Pré-requis
Plateforme	Les plateformes 32-bits **`(IA-32, x86)`** et 64-bits **`(x86-64, x64, amd64)`** **Intel** sont supportées.
Espace disque	Au minimum 512 Mo d'espace disque libre pour les répertoires de **Dr.Web pour Linux**.
OS	**Linux** pour les plateformes **Intel x86/amd64** basées sur un **`noyau`** `en ver. 2.6.37` ou supérieur, et utilisant la bibliothèque **`glibc`** `en ver. 2.13` ou supérieur. Les distributions des **Linux** supportées sont listées ci-dessous. Dans les systèmes fonctionnant sur une plateforme 64-bits, le support des applications 32-bits peut être activé (des bibliothèques additionnelles seront sans doute installées, voir ci-dessous).
Autre	Les connexions réseaux valides suivantes sont requises : Connexion Internet valide pour activer les mises à jour des bases de données virales et les composants de **Dr.Web pour Linux** et pour se connecter à **Dr.Web Cloud** (à condition que l'utilisateur l'a autorisé). En mode Protection centralisée, la connexion au serveur dans le réseau est suffisante ; une connexion Internet n'est pas requise.

Le produit a été testé dans les distributions suivantes de **Linux** (32-bits and 64-bits):

Nom de la distributionLinux	Version	Bibliothèques supplémentaires requises pour les versions 64-bits de l'OS
Debian	7.8	**`libc6-i386`**
Fedora	20, 21	**`glibc.i686`**
Mint	17.1	**`libc6-i386`**
Ubuntu	12.04, 14.04, 14.10	**`libc6-i386`**
CentOS	5.11, 6.6, 7.1	**`glibc.i686`**
Red Hat Enterprise Linux	5.11, 6.6, 7.1	**`glibc.i686`**
SUSE Linux Enterprise Server	11 SP3, 12	–

D'autres distributions de **Linux** qui répondent aux pré-requis n'ont pas été testées pour vérifier la compatibilité avec **Dr.Web pour Linux** mais peuvent être supportées. Si un problème de compatibilité survient, contactez le support technique sur le site official à la page http://support.drweb.com/request/.



Avec **Debian, Fedora, Mint**, et **Ubuntu**, **SpIDer Guard** (voir ci-dessous) utilise l'interface de gestion **`fanotify`** par défaut. Sur **CentOS** et **Red Hat Enterprise Linux**, le composant utilise un module noyau chargeable spécial, qui est fourni complètement construit avec le produit.

Si nécessaire, vous pouvez créer un module chargeable manuellement en utilisant les codes source fournis pour tout système d'exploitation basé sur **GNU/Linux** avec le noyau `2.6.x` et supérieur.

Dans l'OS **SUSE Linux Enterprise Server**, avec les paramètres par défaut, le composant **SpIDer Gate** a des problèmes de compatibilité avec le pare-feu système **SuseFirewall2**. La méthode de la résolution du conflit est décrit dans la rubrique « Description des erreurs connues », voir le conseil sur la récupération de l'erreur avec le code x109.



Packages additionnels

- Pour autoriser le fonctionnement de **Dr.Web pour Linux** en mode graphique et le démarrage du logiciel pour l'installation et la suppression du produit en mode graphique, le sous-système **X Window System** et un gestionnaire de fenêtre sont requis. De plus, pour un fonctionnement correct de l'indicateur pour l'environnement de bureau **Ubuntu Unity**, la bibliothèque **`libappindicator1`** est également requise.
- Pour les scans planifiés, **`crond`** doit être installé dans le système.
- Pour lancer l'installateur ou le désinstallateur du produit en ligne de commande ou en mode graphique, un émulateur de terminal (comme **`xterm`**, **`xvt`**, etc.) est requis. Pour activer l'élévation des privilèges durant l'installation ou la désinstallation, un des utilitaires suivants est requis : **`su`**, **`sudo`**, **`gksu`**, **`gksudo`**, **`kdesu`**, **`kdesudo`**.

Pour travailler correctement avec **Dr.Web pour Linux** en ligne de commande, vous pouvez activer la commande auto-completion dans la commande shell utilisée (si elle est désactivée).



Si vous rencontrez un problème avec l'installation de packages ou composants supplémentaires, référez-vous aux Manuels Utilisateur concernant la distribution utilisée pour le système d'exploitation installé.



Licencing

Les permissions pour utiliser **Dr.Web pour Linux** sont accordées par la *licence* achetée auprès de **Doctor Web** ou auprès des partenaires de **Doctor Web** Les paramètres de la licence déterminant les droits utilisateur sont définis en accord avec le **Contrat de licence** que l'utilisateur accepte durant l'installation du produit. Le Contrat de licence contient des informations concernant l'utilisateur et le vendeur comme les paramètres d'utilisation du produit acheté, incluant :

- La liste des composants licenciés pour l'utilisateur
- La durée de la licence
- D'autres conditions (par exemple, le nombre d'ordinateurs sur lequel **Dr.Web pour Linux** acheté peut être utilisé).

Afin de tester le produit, les utilisateurs doivent activer la *version démo*. Après une activation réussie, la version démo fournit l'ensemble des fonctionnalités du produit pour toute la durée de validité de la démo.

Chaque licence produit **Doctor Web** possède un numéro de série unique associé à un fichier spécifique conservé sur l'ordinateur de l'utilisateur. Ce fichier régule le fonctionnement des composants de **Dr.Web pour Linux** en conformité avec les paramètres de la licence et est nommé fichier clé de *licence*. Lors de l'activation d'une version démo, un fichier clé spécifique, nommé fichier clé de *démo*, est généré automatiquement.

Si aucune licence ni version démo n'est activée sur l'ordinateur, les composants de **Dr.Web pour Linux** sont bloqués. De plus, les mises à jour des bases virales ne peuvent pas être téléchargées sur les serveurs de mise à jour de **Doctor Web**. Mais vous pouvez activer **Dr.Web pour Linux** en le connectant au serveur de protection centralisée comme partie du réseau antivirus administré par l'entreprise ou le fournisseur de services Internet. Dans ce cas, le fonctionnement de **Dr.Web pour Linux** et les mises à jour sont gérés par le serveur de protection centralisée.

Achat et enregistrement des licences

Après l'achat d'une licence, les mises à jour des bases de données virales et des composants sont régulièrement téléchargées depuis les serveurs de mise à jour de **Doctor Web**. De plus, si l'utilisateur a rencontré le moindre problème lors de l'installation ou de l'utilisation du produit acheté, il bénéficie du support technique fourni par **Doctor Web** ou les partenaires de **Doctor Web**.

Vous pouvez acheter n'importe quel produit **Dr.Web** ainsi qu'obtenir un numéro de série pour un produit via la boutique en ligne ou auprès de nos partenaires. Pour en savoir plus sur les durées et les types de licence, visitez le site officiel de **Doctor Web** à la page http://www.drweb.fr/.

L'enregistrement de la licence est requis pour garantir que vous êtes un utilisateur légal de **Dr.Web pour Linux** et activer les fonctionnalités de **Dr.Web pour Linux**, y compris la mise à jour des bases de données virales. Il est recommandé d'enregistrer le produit et d'activer la licence à la fin de l'installation. Une licence achetée peut être activée d'une des façons suivantes :

- via l' Assistant d'enregistrement intégré au **Gestionnaire de licences**.
- sur le site officiel de **Doctor Web** à la page http://products.drweb.com/register/.

Durant l'activation, il est requis d'entrer le numéro de série de la licence achetée. Le numéro de série est fourni avec le produit ou par email lors de l'achat ou du renouvellement de la licence en ligne.





Si vous avez utilisé **Dr.Web pour Linux** par le passé, vous pouvez bénéficier d'une extension de votre nouvelle licence de 150 jours. Pour activer le bonus, entrez votre numéro de série enregistré ou fournissez le fichier clé de licence. Attention, si vous choisissez le renouvellement de licence mais que vous ne fournissez pas les données de la licence précédente, la durée de validité de la nouvelle licence sera amputée de 150 jours.

Si vous possédez plusieurs licences pour utiliser sur plusieurs ordinateurs, mais que vous choisissez d'utiliser le produit sur un seul ordinateur, vous pouvez l'indiquer et la durée de validité de la licence sera automatiquement étendue.

Obtenir une version démo

Les utilisateurs de **Dr.Web** peuvent obtenir une version démo pour

- 3 mois
- 1 mois

Pour obtenir une version démo de trois mois, enregistrez-vous sur le site officiel de **Doctor Web** et indiquez les données requises. Après l'enregistrement, vous recevrez un email contenant un numéro de série pour l'activation de **Dr.Web pour Linux**. La version démo d'un mois peut être obtenue via la fenêtre de l'Assistant d'enregistrement du **Gestionnaire de licences**. Pour obtenir une version démo d'un mois, vous n'avez pas besoin d'indiquer de données personnelles.

L'Assistant d'enregistrement du **Gestionnaire de licences** s'ouvre après le premier démarrage de **Dr.Web pour Linux** (en général, l'Assistant d'enregistrement s'ouvre à la fin de l'installation de **Dr.Web pour Linux**). Vous pouvez démarrer l'enregistrement ou obtenir une version démo depuis la fenêtre du **Gestionnaire de licences** à n'importe quel moment en cliquant sur le bouton **Obtenir une nouvelle licence...** sur la page donnant les informations sur la licence en cours.



Pour activer une licence en utilisant le numéro de série ou demander une version démo, une connexion Internet valide est requise.

Il est possible d'obtenir une autre version démo pour le même ordinateur après un certain délai.

Lorsqu'une version démo ou une licence est activée via le **Gestionnaire de licences**, le fichier clé (licence ou démo) est automatiquement généré sur l'ordinateur local dans le dossier cible. Si vous vous enregistrez sur le site web, le fichier clé est envoyé par email et vous devez installer le fichier clé manuellement.

Enregistrement ultérieur

Si vous avez perdu le fichier clé mais que la licence n'a pas expiré, vous devez vous enregistrer à nouveau en entrant les données que vous aviez fournies lors du premier enregistrement. Vous pouvez utiliser une adresse email différente. Dans ce cas, le fichier clé sera envoyé sur la nouvelle adresse indiquée.

Le nombre de demandes d'un fichier clé est limité. Un numéro de série ne peut pas être enregistré plus de 25 fois. Si un nombre de requêtes supérieur à ce chiffre est envoyé, aucun fichier clé ne sera délivré. Pour recevoir un fichier clé perdu, contactez le Support technique, décrivez votre problème en détails, et indiquez les données que vous avez fournies au moment de l'enregistrement du numéro de série. Le fichier clé de licence sera envoyé par email.

Fichier clé

Le fichier clé est un fichier spécifique conservé sur l'ordinateur local. Il correspond à la licence achetée ou à la version démo activée pour **Dr.Web pour Linux**. Le fichier contient les données sur la licence ou la version démo et les règles d'utilisation de l'une ou de l'autre.

Le fichier clé comporte l'extension `.key` et est valide s'il répond aux critères suivants :

- La licence ou la version démo n'a pas expiré
- La version démo ou la licence s'applique à tous les composants antivirus requis par le produit
- L'intégrité du fichier clé n'a pas été violée

Si une de ces conditions est violée, le fichier clé de licence devient invalide.



Durant le fonctionnement de **Dr.Web pour Linux**, le fichier clé doit résider par défaut dans le dossier `/etc/opt/drweb.com` et posséder le nom **`drweb32.key`**.

Les composants de **Dr.Web pour Linux** vérifient régulièrement que le fichier clé est disponible et valide. Le fichier clé comporte une signature digitale afin de prévenir sa modification. Ainsi, un fichier clé modifié devient invalide. Il n'est pas recommandé d'ouvrir le fichier clé dans des traitements de texte afin d'éviter son invalidation accidentelle.

Si aucun fichier clé valide (licence ou démo) n'est trouvé, ou si la licence a expiré, le fonctionnement des composants antivirus est bloqué jusqu'à ce qu'un fichier clé valide soit installé.

Il est recommandé de conserver le fichier clé de licence jusqu'à son expiration, et de l'utiliser pour réinstaller **Dr.Web pour Linux** ou l'installer sur une autre ordinateur. Dans ce cas, vous devez utiliser le même numéro de série de produit et les mêmes données utilisateur que celles fournies lors de l'enregistrement.

Installation du Fichier Clé

Si vous possédez un fichier clé correspondant à une licence valide pour un produit (par exemple, si vous avez obtenu le fichier clé par email ou si vous souhaitez utiliser **Dr.Web pour Linux** sur un autre ordinateur), vous pouvez activer **Dr.Web pour Linux** en indiquant le chemin vers le fichier clé.

Vous pouvez indiquer le chemin du fichier clé

- Dans le **Gestionnaire de licences** en cliquant sur **Autres types d'activation** à la première étape de la procédure d'enregistrement et en indiquant le chemin du fichier clé.
- Manuellement. Pour cela
  1. Décompressez le fichier clé s'il est dans une archive
  2. Copiez le fichier dans le dossier `/etc/opt/drweb.com` et renommez-le ainsi **`drweb32.key`**

Vous pouvez également utiliser la commande suivante :

```
$ drweb-ctl cfset Root.KeyPath </path/to/key/file>
```

Dans ce cas, le fichier clé ne sera pas copié dans le dossier `/etc/opt/drweb.com` et restera à son emplacement d'origine. Si c'est le cas, l'utilisateur doit s'assurer que le fichier est protégé contre la corruption ou la suppression. Cette méthode d'installation n'est pas recommandée car le fichier clé peut être accidentellement supprimé du système (par exemple, si le dossier où le fichier clé réside est régulièrement nettoyé).



Fichier de configuration de la connexion

Le fichier de configuration de la connexion est un fichier spécifique qui conserve les paramètres de configuration de la connexion entre **Dr.Web pour Linux** et le serveur de protection centralisée.

Ce fichier est fourni par l'administrateur du réseau antivirus ou le fournisseur de service Internet (si ce dernier fournit le support du service de protection antivirus centralisée).

Vous pouvez utiliser ce fichier pour activer **Dr.Web pour Linux** au moment de sa connexion avec le serveur de protection centralisée (dans ce cas, vous ne pouvez pas utiliser **Dr.Web pour Linux** en mode stand-alone sans acheter une licence supplémentaire).

Activation via la connexion au serveur de protection centralisée

Si le fournisseur de service Internet ou l'administrateur réseau a fourni un fichier contenant les paramètres de connexion au serveur de protection centralisée, vous pouvez activer **Dr.Web pour Linux** en indiquant le chemin vers ce fichier.

Pour indiquer le chemin vers le fichier de configuration de la connexion

1. Ouvrez le **Gestionnaire de licences** et démarrez la procédure d'enregistrement en cliquant sur le bouton **Obtenir une nouvelle licence...**
2. Sélectionnez **Autres types d'activation**.
3. Indiquez le chemin du fichier dans la boîte de dialogue qui s'affiche.



Installer et supprimer Dr.Web pour Linux

Cette section décrit comment installer, mettre à jour et supprimer **Dr.Web pour Linux** en version 10.1.0. Dans ce chapitre, vous trouverez également la procédure de mise à niveau vers une nouvelle version, si **Dr.Web pour Linux** de la version antérieure est déjà installé sur votre ordinateur.

Ces procédures peuvent être effectuées uniquement par un utilisateur possédant les privilèges administrateur (superuser `root`). Pour élever les privilèges, utilisez la commande **`su`** (modifier l'utilisateur en cours) ou la commande **`sudo`** (exécuter la commande indiquée avec les privilèges d'un autre utilisateur).

Mise à nouveau vers une Nouvelle Version

Remarques préalables

La procédure de mise à niveau à la version 10.1.0 est uniquement prise en charge pour les versions 9.0 et 10.0. Notez que votre version de **Dr.Web pour Linux** doit être mise à niveau comme elle a été installée

- Si la version actuelle a été installée depuis le dépôt, la mise à niveau requiert la mise à jour des packages depuis le dépôt.
- Si la version actuelle a été installée depuis la distribution, la mise à niveau requiert l'installation d'une nouvelle distribution (correspondant à la nouvelle version) .



Pour identifier la façon dont a été installé le produit, vérifiez que le répertoire de l'exécutable de **Dr.Web pour Linux** (`/opt/drweb` ou `/opt/drweb.com/bin`, en fonction de la version du produit) contient **`remove.sh`** delete script. Si c'est le cas, la version actuelle a été installée depuis le package universel ; sinon, elle a été installée depuis le dépôt.

Si vous ne pouvez pas mettre à niveau le produit comme vous l'avez installé, supprimez la version actuelle de **Dr.Web pour Linux** puis installez une nouvelle version en utilisant la méthode qui vous convient. Les procédures d'installation et de suppression des versions antérieures de **Dr.Web pour Linux** sont les mêmes que les procédures installation et suppression décrites dans le manuel actuel pour la version 10.1.0. Pour en savoir plus, consultez le Manuel Utilisateur correspondant à votre version actuelle de **Dr.Web pour Linux**.



Notez que pour migrer de **Dr.Web pour Linux** de la version 6.0.2 vers la version 10.1.0 **il vous faudra** supprimer le produit de la version 6.0.2 et puis installer le produit de la version 10.1.0.

Mise à niveau version 9.0 et plus récent

Installer un package universel pour une mise à niveau

Installez **Dr.Web pour Linux** 10.1.0depuis le fichier d'installation. Durant l'installation, vous serez invité à supprimer automatiquement l'ancienne version si c'est nécessaire.

Mettre à niveau depuis le dépôt

Pour mettre à niveau votre version actuelle de **Dr.Web pour Linux** installée depuis le dépôt de **Doctor Web**, en fonction des types de packages, faite comme suit:

- **Si vous utilisez des packages RPM (yum):**

  1. Supprimez tous les packages de la version actuelle en utilisant la commande

     ```
     # yum remove drweb*
     ```

     Dans certains systèmes d'exploitation, le symbole '*' doit être évité. Dans ce cas, indiquez

drweb* au lieu de drweb*. Cette commande vous invitera à supprimer **tous** les packages **Dr.Web** installés. Par conséquent, elle doit être utilisée avec prudence si vous avez installé plusieurs produits **Dr.Web** sur votre poste de travail.

2. Modifiez le dépôt utilisé (du dépôt du package de votre version actuelle vers le dépôt du package 10.1.0).



Vous pouvez trouver le nom du dépôt au chapitre Installer depuis el dépôt de Dr.Web. Pour en savoir plus sur la façon de modifier les dépôts, consultez les aides du système d'exploitation utilisé.

3. Installez la nouvelle version de **Dr.Web pour Linux** en utilisant la commande

```
# yum install drweb-workstations
```

Pour en savoir plus, consultez les chapitres Supprimer et Installer les packages produits en utilisant le dépôt de **Dr.Web** (les parties correspondant à l'OS et au gestionnaire de packages utilisés).

- **Si vous utilisez des packages DEB (apt-get):**

1. Modifiez le dépôt utilisé (du dépôt du package de votre version actuelle vers le dépôt du package 10.1.0).

2. Mettez à niveau le produit en utilisant la commande suivante :

```
# apt-get update
# apt-get dist-upgrade
```

Transfert du fichier clé de licence

Quelle que soit la méthode de mise à niveau de **Dr.Web pour Linux**, le fichier clé de licence est installé dans un emplacement par défaut.

Caractéristiques du processus de mise à niveau

- Notez que si votre version actuelle de **Dr.Web pour Linux** est active au moment de la mise à niveau, les processus de l'ancienne version continuent à être exécutés jusqu'à ce que l'utilisateur quitte le système après la fin de la mise à niveau. Ainsi, si opère **Dr.Web pour Linux** en mode graphique, l'icône de l'ancienne version peut s'afficher dans la zone de notifications.
- Après la mise à niveau de **Dr.Web pour Linux** 10.0 vers la version 10.1 les paramètres de **SpIDer Gate** seront réinitialisés aux valeurs par défaut.

Mise à niveau de la version 6.0.2 et les versions antérieures

Migrer de **Dr.Web pour Linux** de la version 6.0.2 et antérieures vers la version 10.1.0 il vous faudra supprimer le produit de la antérieures version et puis installer le produit de la version 10.1.0. Pour des informations sur la suppression, consultez le Manuel Utilisateur correspondant à antérieures version de **Dr.Web pour Linux**.

Transfert du fichier clé de licence

Le fichier clé de licence ne est pas installé dans un emplacement par défaut. Vous pouvez l'installer manuellement. Le fichier clé pour la version 6.0.2 et antérieures réside dans répertoire /home/<user>/.drweb (répertoire est caché). Si un fichier clé valide est perdu, contactez le support technique de **Doctor Web**.





Dr.Web pour Linux 10.1.0 ne supporte pas la quarantaine de **Dr.Web pour Linux** 6.0.2 ! Si des fichiers isolés demeurent dans la quarantaine d'une ancienne version, vous pouvez récupérer ou supprimer ces fichiers manuellement. La quarantaine de **Dr.Web pour Linux** 6.0.2 isole les fichiers dans les répertoires suivants :

- `/var/drweb/infected` – system
- `/home/<user>/.drweb/quarantine` – utilisateur (où `<user>` est le nom de l'utilisateur).

Pour simplifier le traitement des fichiers placés en quarantaine, il est recommandé de revoir l'utilisation de la quarantaine avec **Dr.Web pour Linux** 6.0.2 avant de commencer la mise à niveau.

Procédure d'Installation

Pour installer **Dr.Web pour Linux**, effectuez une des actions suivantes:

- Téléchargez le fichier d'installation grâce au package universel pour les systèmes UNIX sur le site officiel de **Doctor Web**. Le package est fourni avec les installateurs (graphique et console) démarrant en fonction de l'environnement.
- Téléchargez les packages natifs depuis le dépôt du package de **Doctor Web** correspondant.



Quel que soit le mode d'installation de **Dr.Web pour Linux** sélectionné, après la fin de l'installation, vous devez soit activer la licence, soit installer le fichier clé si vous l'avez obtenu, ou connecter **Dr.Web pour Linux** au serveur de protection centralisée.

Tant que vous n'aurez pas fait cela, **la protection antivirus sera désactivée.**

Installer le Package Universel

Dr.Web pour Linux est distribué sous forme de fichier d'installation nommé **`drweb-workstations_<version>~linux_<platform>.run`**, où **`<version>`** est une ligne qui contient la version et la période de sortie du produit et **`<platfrom>`** est la plateforme pour laquelle le produit est prévu (**`x86`** pour les plateformes 32-bits, **`amd64`** pour les plateformes 64-bits). Par exemple:

```
drweb-workstations_10.1.0.0-1501012000~linux_x86.run
```

Notez que le nom du fichier d'installation correspondant au format susmentionné s'y réfère sous la forme **`<nom_de_fichier>.run`**.

Pour installer les composants de **Dr.Web pour Linux**

1. Téléchargez l'archive sur le site officiel de **Doctor Web**.
2. Sauvegardez l'archive sur le disque dur de l'ordinateur.
3. Autorisez l'archive à s'exécuter en utilisant par exemple la commande suivante :

   ```
   # chmod +x }<nom_de_fichier>.run
   ```

4. Exécutez l'archive en utilisant la commande suivante :

   ```
   # ./<nom_de_fichier>.run
   ```

   ou utilisez le gestionnaire de fichier standard de l'interface graphique pour modifier les propriétés du fichier et exécuter le fichier.

   Ainsi, l'intégrité de l'archive d'installation est vérifiée puis un ensemble de fichiers sont extraits de cette archive et placés dans un dossier temporaire et la procédure d'installation est lancée



automatiquement. S’il n’est pas lancé avec les privilèges `root`, le programme d’installation tente d’élever les privilèges en utilisant **sudo**. Si cette étape échoue, l’installation s’arrête.

En fonction de l’environnement dans lequel la distribution est lancée, un des programmes d’installation suivants s’exécute :

- Assistant d’Installation pour le mode graphique
- Installateur pour le mode ligne de commande

Ainsi, l’installateur pour le mode ligne de commande est automatiquement lancé si l’Assistant d’Installation pour le mode graphique échoue à démarrer.

5. Suivez les requêtes de l’installateur.



Notez que si la distribution de **Linux** inclut **SELinux**, le processus d’installation peut être interrompu par le sous-système de sécurité. Si une telle situation arrive, passez **SELinux** en mode `(Permissive)`. Pour cela, entrez la commande suivante :

```
# setenforce 0
```

et redémarrez l’installateur.

Après la fin de l’installation, configurez les politiques de sécurité de **SELinux** pour permettre un fonctionnement correct des composants de **Dr.Web pour Linux**.

Tous les fichiers d’installation extraits seront automatiquement supprimés à la fin de l’installation.

Une fois l’installation achevée, l’onglet **Dr.Web** s’affiche dans le menu du logiciel dans l’interface graphique du bureau. Cet élément en contient deux autres :

- **Dr.Web pour Linux** pour lancer **Dr.Web pour Linux** en mode graphique
- L’élément **Supprimer les composants de Dr.Web** pour supprimer les composants

L’icône de l’indicateur de statut du programme est affichée automatiquement dans la zone de notifications du bureau après la reconnexion de l’utilisateur au système.



Notez que l’installation des paquets, indiqués dans la rubrique Pré-requis système peut être requise pour le fonctionnement correct de **Dr.Web pour Linux** (par exemple, l’installation de la bibliothèque de support des applications 32-bits pour la platform 64-bits ou la bibliothèque **libappindicator1** pour l’affichage correct de l’indicateur de statut du programme dans la zone de notifications du bureau).

Si nécessaire, vous pouvez profiter de l’option Installation personnalisée (par exemple, pour réparer des erreurs survenues dans le fonctionnement de **Dr.Web pour Linux**).

Installation en Mode Graphique

Si, au début de son fonctionnement, le programme d’installation détecte des problèmes qui pourraient mettre **Dr.Web pour Linux** en état non opérationnel complet ou partiel, une liste de problèmes détectés sera affichée dans une fenêtre correspondante. Pour résoudre les problèmes détectés avant l’installation, veuillez interrompre l'installation en cliquant sur **Sortie**. Dans ce cas vous devez relancer le programme d’installation après la résolution des problèmes détectés (installation des bibliothèques requises, désactivation temporaire de **SELinux**, etc.). Pour ne pas interrompre l’installation de **Dr.Web pour Linux**, cliquez sur **Continuer**. Dans ce cas, l’installation sera poursuivie et la fenêtre de l’Assistant d’installation sera affichée. Cependant il vous faudra résoudre les problèmes détectés plus tard, après la fin d’installation ou en cas de détection d’erreurs de fonctionnement de **Dr.Web pour Linux**.

Après le démarrage du programme d’installation en mode graphique, la fenêtre de l’Assistant d’Installation s’affiche.



Image 2. Page de bienvenue

Pour installer **Dr.Web pour Linux** sur l'ordinateur, effectuez les actions suivantes:

1. Lisez le **Contrat de Licence** de **Doctor Web**. Pour cela, cliquez sur **Contrat de Licence**. Une page contenant le **Contrat de Licence**et les données de copyright pour les composants installés va s'ouvrir.

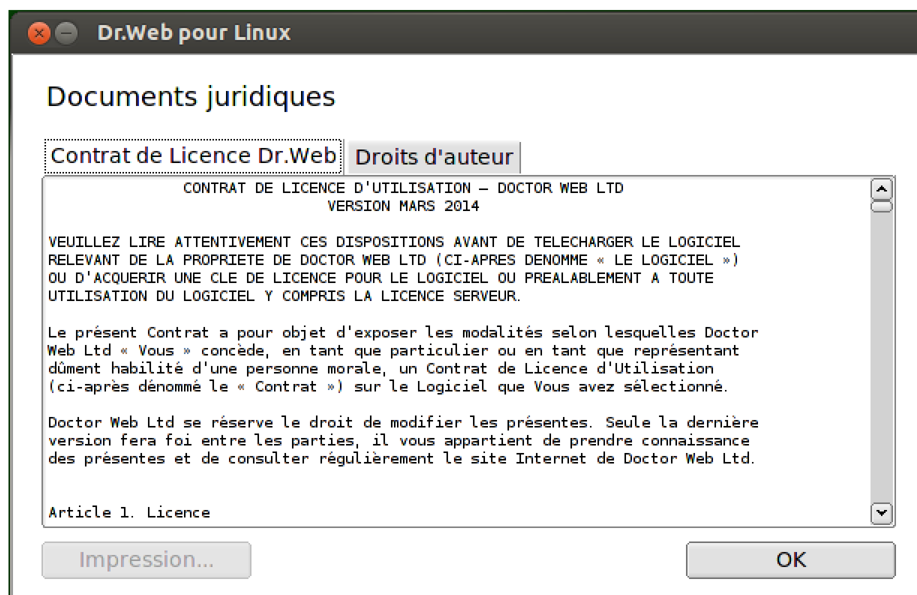


Image 3. Page du Contrat de Licence



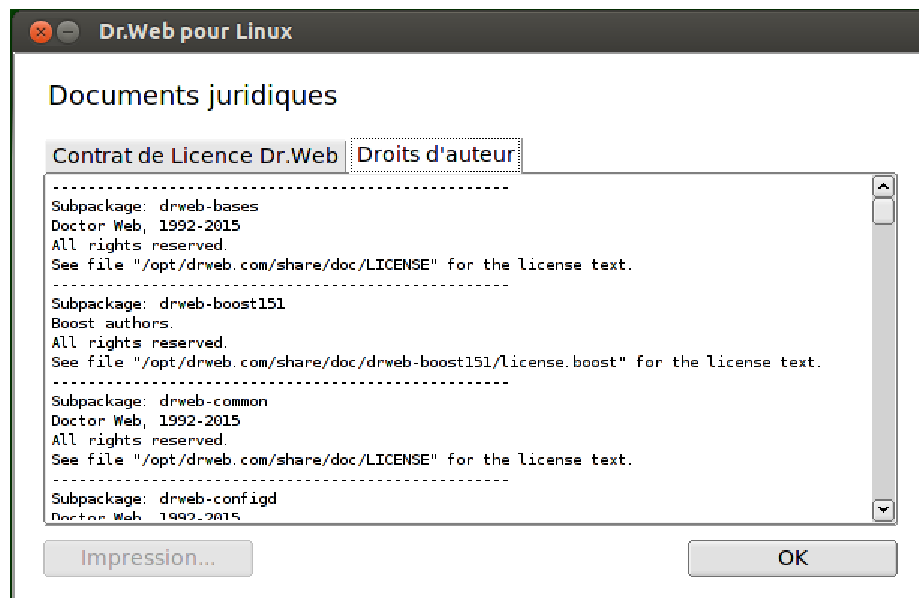


Image 4. Page d'informations sur le copyright

Si nécessaire, vous pouvez imprimer le **Contrat de Licence** et les informations de copyright. Pour cela, ouvrez l'onglet souhaité sur la page du **Contrat de Licence** et cliquez sur **Impression...**.

Pour fermer la page, cliquez sur **OK**.

2. Pour démarrer l'installation, vous pouvez autoriser la connexion automatique au service **Dr.Web Cloud** après l'installation de **Dr.Web pour Linux**. Pour ce faire cochez la case correspondante (la case est cochée par défaut au moment de lancement de l'Assistant d'Installation). Si vous ne voulez pas autoriser **Dr.Web pour Linux** à utiliser le service **Dr.Web Cloud**, décochez la case. Vous pouvez interdire ou autoriser à **Dr.Web pour Linux** d'utiliser le service **Dr.Web Cloud** à tout moment dans les paramètres du logiciel.

3. Pour lancer l'installation cliquez sur le bouton **Installer**. Ainsi vous acceptez les conditions du **Contrat de licence** de **Doctor Web**. Si vous choisissez de ne pas installer **Dr.Web pour Linux** sur votre ordinateur, cliquez sur **Annuler**. Une fois le bouton cliqué, l'Assistant d'Installation quitte. Si vous choisissez d'installer le produit, cliquez sur **Installer**.

4. Après le démarrage de l'installation, une page avec la barre de progression s'ouvre. Si nécessaire, vous pouvez cliquer sur **Afficher les détails** et voir le fichier de log de l'installation.



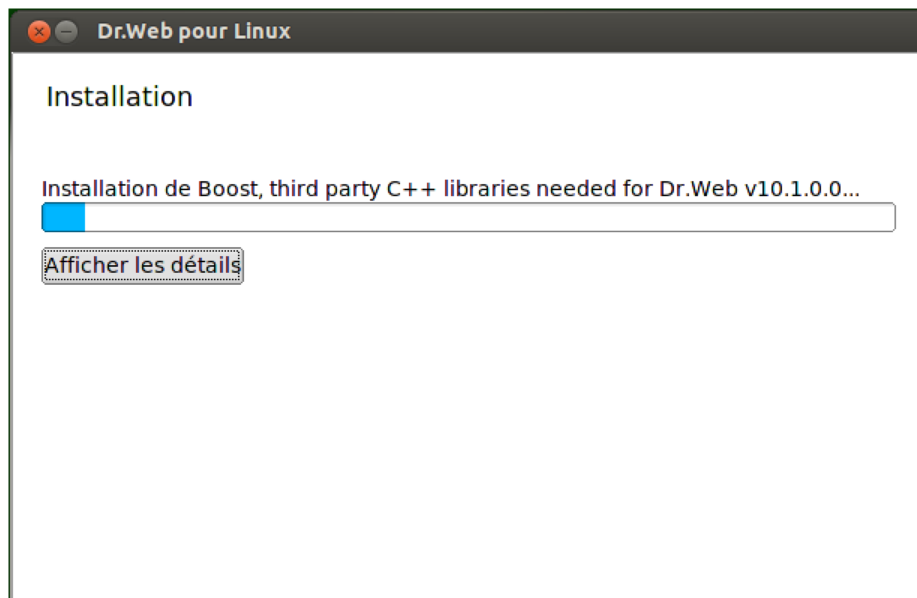


Image 5. Barre de progression de l'installation

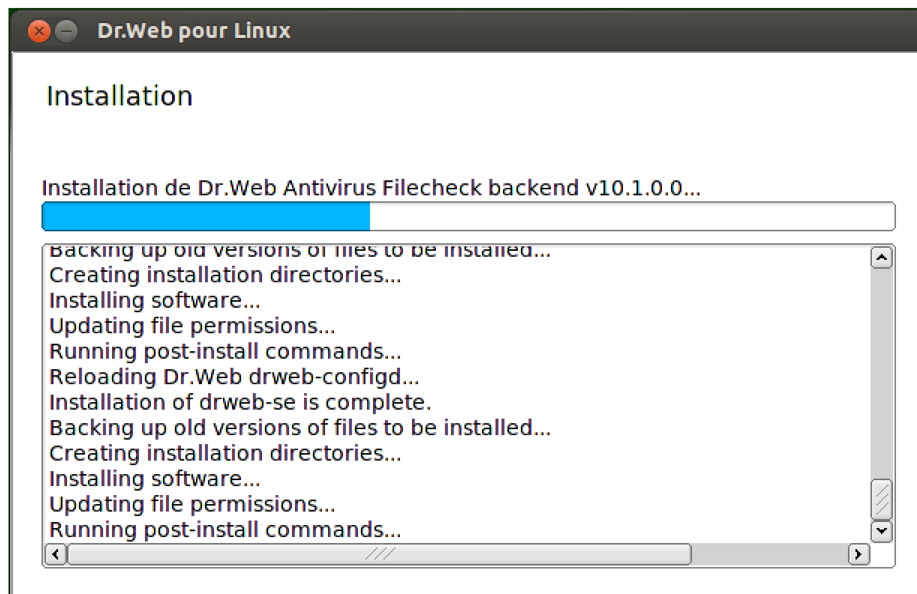


Image 6. Voir le fichier de log de l'installation

5. Une fois les fichiers du logiciel copiés avec succès et les réglages du système de fichiers effectués, la dernière page donnant les résultats de l'installation s'affiche.



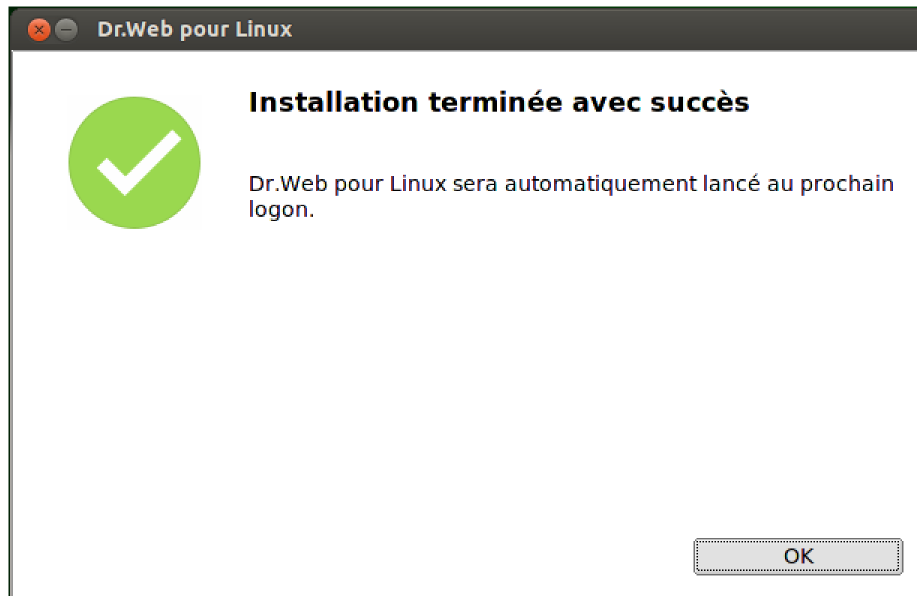


Image 7. Page des résultats de l'installation

6. Pour quitter l'Assistant d'Installation, cliquez sur **OK.** Si cette operation est supportée par l'ordinateur, à l'étape finale une page s'affichera proposant de lancer **Dr.Web pour Linux** en mode graphique. Pour lancer, cochez la case **Lancer Dr.Web pour Linux maintenant** et cliquez sur **OK**.

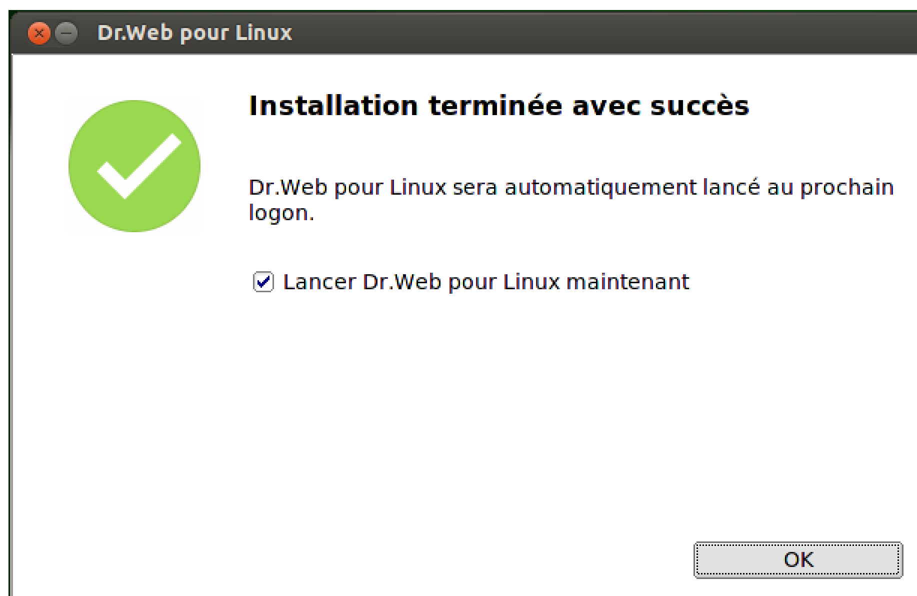


Image 8. Proposition de lancer Dr.Web pour Linux après l'installation

Si le processus d'installation échoue à cause d'une erreur, la dernière page de l'Assistant d'Installation contiendra un message correspondant. Dans ce cas, sortez de l'Assistant d'Installation, résolvez le problème qui a provoqué l'erreur et démarrez une nouvelle procédure d'installation.

Installation en Ligne de Commande

Lorsque le programme d'installation pour la ligne de commande démarre, l'invite de commandes s'affiche sur l'écran.

1. Pour démarrer l'installation, entrez `Yes` ou `Y` en réponse à la question "Souhaitez-vous continuer ?".

Pour sortir de l'installateur, entrez `No` ou `N`. Dans ce cas, l'installation est annulée.

```
Terminal
root@userm:/home/user/drweb-workstations_10.1.0.0-1501081632~linux_x86# ./setup.sh

Ce script d'installation vous aidera à installer Dr.Web pour Linux

Vous voulez continuer ? (YES/no) _
```

Image 9. Invite de commandes pour installer le produit

2. Ensuite, vous devez lire le **Contrat de Licence** de **Doctor Web** qui s'affiche sur l'écran. Appuyez sur ENTREE pour descendre ligne par ligne ou sur LA BARRE D'ESPACE pour passer à la page suivante. Notez que les options pour consulter le texte du **Contrat de Licence** ligne par ligne ou page par page ne sont pas disponibles.

```
Terminal
                CONTRAT DE LICENCE D'UTILISATION – DOCTOR WEB LTD
                                VERSION MARS 2014

VEUILLEZ LIRE ATTENTIVEMENT CES DISPOSITIONS AVANT DE TELECHARGER LE LOGICIEL
RELEVANT DE LA PROPRIETE DE DOCTOR WEB LTD (CI-APRES DENOMME « LE LOGICIEL »)
OU D'ACQUERIR UNE CLE DE LICENCE POUR LE LOGICIEL OU PREALABLEMENT A TOUTE
UTILISATION DU LOGICIEL Y COMPRIS LA LICENCE SERVEUR.

Le présent Contrat a pour objet d'exposer les modalités selon lesquelles Doctor
Web Ltd « Vous » concède, en tant que particulier ou en tant que représentant
dûment habilité d'une personne morale, un Contrat de Licence d'Utilisation
(ci-après dénommé le « Contrat ») sur le Logiciel que Vous avez sélectionné.

Doctor Web Ltd se réserve le droit de modifier les présentes. Seule la dernière
version fera foi entre les parties, il vous appartient de prendre connaissance
des présentes et de consulter régulièrement le site Internet de Doctor Web Ltd.


Article 1. Licence

1.1 Octroi de licence

Ce contrat de souscription de licence d'Utilisation Vous permet de disposer de
certains droits limités d'utilisation du Logiciel sous forme de code objet
pendant la période de souscription de la licence définie à l'article 2 des
Présentes. Le Logiciel comprend l'ensemble de ses fonctions et services et sa
documentation, y compris l'emballage du produit. Etant entendu que Doctor Web
Ltd reste toujours propriétaire du Logiciel, il n'y a donc aucun transfert de
propriété du Logiciel.

Le fait de cliquer sur le bouton ou de cocher la case « J'accepte le Contrat »
sur le site de Doctor Web Ltd ou d'un distributeur agréé, ou d'installer la clé
--Plus--(6%)
```

Image 10. Lire le Contrat de Licence



3. Après avoir lu le **Contrat de Licence**, vous êtes invité à l'accepter. Tapez **Yes** ou **Y** si vous acceptez le **Contrat de Licence**. Si vous refusez de l'accepter, tapez **No** ou **N**. Dans ce cas, l'installateur quitte.

```
Terminal
part à l'une des dispositions du présent Contrat de Licence. Vous devrez alors
cesser toute utilisation du Logiciel et détruire tous les exemplaires du
Logiciel en votre possession ainsi que sa documentation. Le fichier clé dont
Vous disposerez sera par ailleurs automatiquement désactivé.


7.2 Résiliation unilatérale du Client

Dans le cadre du présent Contrat, vos droits et obligations concernant
l'utilisation de ce Logiciel peuvent être unilatéralement modifiés par Doctor
Web Ltd à condition de Vous en tenir informé au moins UN (1) mois avant leur
entrée en vigueur par mail. Vous bénéficiez d'un délai de QUATRE (4) mois après
l'entrée en vigueur de la modification, tant que Vous n'avez pas expressément
accepté ces nouvelles conditions, pour résilier le Contrat sans pénalité de
résiliation et sans droit à dédommagement pour Doctor Web Ltd.


Article 8. Politique de confidentialité - Règlement amiable et Droit applicable

Vous vous engagez à prendre connaissance et à respecter la politique de gestion
de la confidentialité accessible à l'adresse suivante
http://company.drweb.com/policy/).

Vous vous engagez, dans le cadre d'un désaccord, à procéder à une tentative de
règlement amiable avec Doctor Web Ltd avant tout recours en justice.

En cas de nullité d'une disposition quelconque de ce Contrat, Vous convenez que
les autres dispositions du Contrat n'en seront pas affectées.

Le présent Contrat est régi par le droit national. Tout litige entre Vous et
Doctor Web Ltd sera porté devant le Tribunal compétent relevant du siège social
de la société.

Vous acceptez les termes du Contrat de licence ? (yes/NO) _
```

Image 11. Accepter le Contrat de Licence

4. Après avoir accepté le **Contrat de Licence**, l'installation démarre automatiquement. Durant la procédure, des informations sur le processus d'installation, incluant la liste des composants installés, seront affichées sur l'écran

```
Terminal
Doctor Web, 1992-2015
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
---------------------------------------------------
Subpackage: drweb-spider
Doctor Web, 1992-2015
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
---------------------------------------------------
Subpackage: drweb-update
Doctor Web, 1992-2015
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
---------------------------------------------------
Subpackage: drweb-workstations-doc
Doctor Web, 1992-2015
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
---------------------------------------------------

Doctor Web, 1992-2015
En utilisant ce paramètre, vous acceptez le Contrat de licence.
La dernière version du composant drweb-libs est installée dans le système.
_
```

Image 12. Log de l'installation

5. Une fois l'installation effectuée avec succès, un message correspondant s'affiche sur l'écran et



l'installateur quitte. Si une erreur survient, un message la décrivant s'affiche et l'installateur quitte.

```
Terminal
Répertoires d'installation sont en cours de création...
Installation du composant en cours...
Mise à jour des droits d'accès aux fichiers...
Fin d'installation...
Reloading Dr.Web drweb-configd...
Installation de drweb-spider terminée.
Doctor Web, 1992-2015
En utilisant ce paramètre, vous acceptez le Contrat de licence.
La dernière version du composant drweb-esagent est installée dans le système.
Doctor Web, 1992-2015
En utilisant ce paramètre, vous acceptez le Contrat de licence.
La dernière version du composant drweb-update est installée dans le système.
Doctor Web, 1992-2015
En utilisant ce paramètre, vous acceptez le Contrat de licence.
La dernière version du composant drweb-gui est installée dans le système.
Doctor Web, 1992-2015
En utilisant ce paramètre, vous acceptez le Contrat de licence.
La dernière version du composant drweb-workstations-doc est installée dans le systèm
e.


If SELinux is installed in your system, please see the readme.selinux file or refer
to User manual.
root@userm:/home/user/drweb-workstations_10.1.0.0-1501081632~linux_x86# _
```

Image 13. Message de réussite de l'installation

6. Pour commencer à travailler avec **Dr.Web pour Linux** installé, lancez le produit dans un des modes disponibles.

Si le processus d'installation a échoué à cause d'une erreur, résolvez les problèmes qui l'ont provoquée et démarrez une nouvelle procédure d'installation.

Installation Personnalisée

Décompression du fichier d'installation

Pour démarrer une installation personnalisée, décompressez le fichier d'installation **<nom_de_fichier>.run** sans lancer l'installation du produit. Pour cela, utilisez le paramètre en ligne de commande `--noexec` :

```
# ./< nom_de_fichier>.run --noexec
```

Après l'exécution de la commande, le sous-répertoire `<file_name>` apparaît dans le répertoire courant.

De plus, vous pouvez utiliser les paramètres en ligne de commande suivants avec le fichier d'installation :

`--keep` – créer le répertoire `<file_name>` contenant les fichiers d'installation dans le répertoire courant (non dans `/tmp`), et ne pas le supprimer à la fin de l'installation.

`--target <path_to_dir>` – créer le répertoire `<file_name>` contenant les fichiers d'installation dans un répertoire spécifique. Notez que ce répertoire sera automatiquement supprimé à la fin de l'installation si vous ne précisez pas également le paramètre en ligne de commande `--keep` ou `--noexec`.

Pour voir la liste complète des paramètres en ligne de commande disponibles autorisés pour le fichier d'installation, exécutez la commande

```
$ ./<file_name>.run --help
```



Installation personnalisée des composants

Le sous-répertoire créé est un répertoire d'installation qui contient des fichiers auxiliaires et tous les packages des composants intégrés à **Dr.Web pour Linux**. Chaque package de composant **<component_name>** contient deux fichiers : `<component_name>.install` et `<component_name>.remove`. Ces fichiers sont des scripts de commande. Le premier script est utilisé pour l'installation du package et le second permet la suppression du package. Les noms de tous les packages contenant les composants de **Dr.Web pour Linux** commencent par le préfixe "`drweb`".

Pour installer un composant en particulier, exécutez le fichier d'installation correspondant dans la console (ou l'émulateur de console qui est un terminal pour le mode graphique).



Pour exécuter un script d'installation pour tout composant, les privilèges administrateur (root) sont requis. Pour obtenir les privilèges root, vous pouvez utiliser soit la commande **su** pour passer à un autre utilisateur, soit la commande **sudo** pour effectuer une action en tant qu'utilisateur différent.

Lors de l'installation de tout composant produit, les dépendances sont supportées ; ainsi, si l'installation d'un composant requiert d'autres composants, leur présence dans le système est vérifiée et, si ce n'est pas le cas, ils sont installés automatiquement.

S'il est nécessaire de lancer l'installation complète du produit, lancez le script d'installation du répertoire extrait. Pour cela, utilisez la commande suivante :

```
$ ./install.sh
```

Installation depuis le Dépôt Dr.Web

Les packages natifs de **Dr.Web pour Linux** sont stockés dans le dépôt officiel de **Dr.Web** à la page http://repo.drweb.com/drweb/. Après avoir ajouté le dépôt **Dr.Web** à la liste de ceux utilisés par le gestionnaire de package de votre système d'exploitation, vous pouvez installer le produit depuis les packages natifs comme vous installez n'importe quel autre programme depuis les dépôts du système d'exploitation. Les dépendances requises sont automatiquement résolues.



Toutes les commandes mentionnées ci-dessous pour la connexion aux dépôts, l'import des clés de signatures numériques, l'installation et la suppression des packages, doivent être effectuées avec les privilèges administrateur (`root`). Pour élever les privilèges, utilisez la commande **su** (modifier l'utilisateur en cours) ou la commande **sudo** (exécuter la commande indiquée avec les privilèges d'un autre utilisateur).

Debian, Ubuntu (apt)

Le dépôt pour ces systèmes d'exploitation est signé numériquement. Pour permettre un fonctionnement correct, importez une clé de signature numérique en utilisant la commande suivante :

```
# wget -O - http://repo.drweb.com/drweb/drweb.key | apt-key add -
```

ou

```
# curl http://repo.drweb.com/drweb/drweb.key | apt-key add -
```

Pour vous connecter au dépôt, ajoutez la ligne suivante au fichier `/etc/apt/sources.list` :

```
# deb http://repo.drweb.com/drweb/debian 10.0.0 non-free
```



En plus de cela, vous pouvez obtenir la clé automatiquement et vous connecter au dépôt de la version 10.1.0 via le téléchargement et l'installation d'un paquet DEB spécial. Lien pour télécharger le package : http://repo.drweb.com/drweb-repo10.deb.

Pour installer **Dr.Web pour Linux** depuis le dépôt, utilisez les commandes suivantes :

```
# apt-get update
# apt-get install drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de packages alternatifs (par exemple, **Synaptic** ou **aptitude**) pour installer le produit. De plus, il est recommandé d'utiliser des gestionnaires alternatifs, comme **aptitude**, pour résoudre un conflit de package s'il survient.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

Ajoutez le fichier avec le contenu mentionné ci-dessous au répertoire `/etc/yum.repos.d` :

Pour les versions 32-bits

```
[drweb]
name=DrWeb - 10.0.0
baseurl=http://repo.drweb.com/drweb/el5/10.0.0/i386/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

Pour les versions 64-bits

```
[drweb]
name=DrWeb - 10.0.0
baseurl=http://repo.drweb.com/drweb/el5/10.0.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

En plus de cela, vous pouvez vous connecter au dépôt de la version 10.1.0 via le téléchargement et l'installation d'un paquet RPM spécial. Lien pour télécharger le package : http://repo.drweb.com/drweb-repo10.rpm.

Pour installer **Dr.Web pour Linux** depuis le dépôt, utilisez la commande suivante :

```
# yum install drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de packages alternatifs (par exemple, **PackageKit** or **Yumex**) pour installer le produit.

Réglage des Politiques SELinux

Si la distribution utilisée de **Linux** inclut **SELinux** (`Linux` sécurisé), vous devrez peut-être configurer les politiques de sécurité de **SELinux** pour permettre un fonctionnement correct des composants (par exemple, le fonctionnement du moteur de scan) après leur installation.

1. Problèmes d'installation du package universel

Si **SELinux** est autorisé, l'installation depuis le fichier d'installation `(.run)` peut échouer parce que la tentative de création de l'utilisateur `drweb`, sous lequel les composants de **Dr.Web pour Linux** fonctionnent, peut être bloquée.

En cas d'échec, vérifiez le mode opératoire de **SELinux** via la commande **getenforce**. La commande affiche un des modes suivants:

* **Permissif** – la protection est active mais une stratégie permissive est mise en place : les actions qui violent la politique de sécurité ne sont pas rejetées mais les informations sur ces actions sont journalisées.
* **Restrictif** – la protection est active et une stratégie restrictive est mise en place : les actions qui violent les politiques de sécurité sont bloquées et les informations sur ces actions sont journalisées.
* **Désactivé** – **SELinux** est installé mais non actif.

Si **SELinux** opère en mode `Restrictif`, passez en mode `Permissif` pour la durée d'installation du produit. Pour cela, utilisez la commande **setenforce 0** qui autorise temporairement (jusqu'au prochain redémarrage) le mode `Permissif` pour **SELinux**.



Notez que quel que soit le mode opératoire autorisé via la commande **setenforce**, le redémarrage du système d'exploitation replace **SELinux** dans le mode opératoire indiqué dans les paramètres de **SELinux** (le fichier des paramètres de **SELinux** réside généralement dans le répertoire `/etc/selinux`).

Après l'installation réussie du produit, activez de nouveau le mode `Restrictif` pour **SELinux** avant de lancer le produit. Pour cela, utilisez la commande **setenforce1**.

2. Problèmes de fonctionnement

Dans certains cas, lorsque **SELinux** est autorisé, certains modules auxiliaires de **Dr.Web pour Linux** (par exemple **drweb-se** et **drweb-filecheck** utilisés par le **Scanner**) ne peuvent pas démarrer. Si c'est le cas, le scan des objets et la surveillance du système de fichiers deviennent indisponibles. Lorsqu'un module auxiliaire échoue à démarrer, la fenêtre principale de **Dr.Web pour Linux** affiche des messages sur les erreurs `119` et `120` et des informations sur ces erreurs sont également enregistrées par **syslog** (le log est généralement placé dans le répertoire `/var/log/`).



Les messages sur les erreurs 119 et 120 peuvent également désigner une tentative de démarrer **Dr.Web pour Linux** dans une version 64-bits du système d'exploitation si la bibliothèque de support de l'application 32-bits est manquante (voir Pré-requis système).

Les messages de **SELinux** sont enregistrés dans les logs du système. En général, lorsque le daemon **audit** est utilisé dans le système, le fichier de log audit est `/var/log/audit/audit.log`. Sinon, les messages sur les opérations bloquées sont sauvegardés dans le fichier de log général dans `/var/log/messages`.



Notez que certaines distributions de **Linux** ne fournissent pas les utilitaires mentionnés ci-dessous. Si c'est le cas, vous pouvez avoir besoin de packages supplémentaires pour ces utilitaires.

Pour créer les politiques requises

1. Créez un nouveau fichier avec le code source de la politique **SELinux** (`.te`). Ce fichier définit les restrictions appliquées au module. Le code source de la politique peut être indiqué d'une des façons suivantes :

   1) **En utilisant** l'utilitaire **audit2allow**, qui est la méthode la plus simple. L'utilitaire génère des règles permissives depuis les messages de déni d'accès dans les fichiers de log du système. Vous pouvez paramétrer de rechercher les messages automatiquement ou indiquer un chemin vers le fichier de log manuellement.

   Notez que vous pouvez utiliser cette méthode uniquement si **Dr.Web pour Linux** a violé les politiques de sécurité de **SELinux** et que ces événements sont enregistrés dans le fichier de log audit. Si ce n'est pas le cas, attendez qu'un incident survienne ou créez de force des



politiques permissives en utilisant l'utilitaire **policygentool** (voir ci-dessous).



L'utilitaire **audit2allow** réside dans le package `policycoreutils-python` ou `policycoreutils-devel` (pour les systèmes d'exploitation **RedHat Enterprise Linux, CentOS, Fedora** en fonction de la version) ou dans le package `python-sepolgen` (pour les OS **Debian, Ubuntu**).

Veuillez noter que pour la version 20 de **Fedora**, il est requis d'installer en plus le package `checkpolicy`, sinon l'utilitaire **audit2allow** remonte une erreur.

Exemple d'Utilisation :

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

Dans l'exemple donné, l'utilitaire **audit2allow** effectue une recherche dans le fichier `audit.log`pour trouver les messages de déni d'accès pour le module **drweb-se**.

Les deux fichiers suivants sont créés : le fichier source de la politique `drweb-se.te` et le module de la politique `drweb-se.pp` prêt à l'installation.

Si aucun incident de violation de la sécurité n'est trouvé dans le log audit du système, l'utilitaire remonte un message d'erreur.

Dans la plupart des cas, vous n'avez pas besoin de modifier le fichier de la politique créé par l'utilitaire. Par conséquent, il est recommandé d'aller à l'étape 4 pour installer le module de la politique `drweb-se.pp`. Notez que l'utilitaire **audit2allow** affiche l'appel à la commande **semodule**. En copiant ce qui s'affiche en ligne de commande et en l'exécutant, vous terminez l'étape 4. Allez à l'étape 2 seulement si vous souhaitez modifier les politiques de sécurité qui ont été automatiquement générées pour les composants de **Dr.Web pour Linux**.

2) **Utiliser l'utilitaire policygentool**. Pour cela, indiquez le nom du module avec lequel vous souhaitez configurer et le chemin complet vers le fichier exécutable.



Notez que l'utilitaire **policygentool**, inclus au package `selinux-policy` pour les OS **RedHat Enterprise Linux** et **CentOS Linux**, peut ne pas fonctionner correctement. Si c'est le cas, utilisez l'utilitaire **audit2allow**.

Exemple de création de politique via policygentool:

- pour **drweb-se** (utilisé par le moteur antivirus) :

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- pour **drweb-filecheck** (utilisé par le **Scanner**):

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Vous serez invité à indiquer plusieurs caractéristiques de domaine commun. Ensuite, trois fichiers déterminant la politique seront créés pour chacun des modules:

`<nom_du_module>.te`, `<nom_du_module>.fc` and `<nom_du_module>.if`.

2. Si nécessaire, modifiez le fichier source de la politique généré `<nom_du_module>.te` puis utilisez l'utilitaire **checkmodule** pour créer un mappage binaire du fichier source de la politique locale (fichier `.mod`).



Notez que pour garantir le succès de la commande, le package `checkpolicy` doit être installé dans le système.



Exemple d'Utilisation

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. Créez un module de politique installé (fichier `.pp`) grâce à l'utilitaire **`semodule_package`**.

   Exemple

```
# semodule_package -o drweb-se.pp -m drweb-se.mod
```

4. Pour installer le module de politique créé, utilisez l'utilitaire **`semodule`**.

   Exemple

```
# semodule -i drweb-se.pp
```

Pour en savoir plus sur le fonctionnement et la configuration de **SELinux**, consultez la documentation sur la distribution de **Linux** utilisée.

Emplacement des Fichiers du Produit

Après l'installation de **Dr.Web pour Linux**, ses fichiers résident dans les répertoires `/opt`, `/etc`, et `/var` du système de fichiers.

La structure des répertoires utilisés se présente comme suit:

Répertoire	Contenu
`/opt/drweb.com/`	Fichiers exécutables des composants du produit et bibliothèques basiques requis pour le fonctionnement de **Dr.Web pour Linux**
`/etc/opt/drweb.com`	Fichiers contenant les paramètres d'un composant (par défaut) et le fichier clé de licence requis pour le fonctionnement de **Dr.Web pour Linux** en mode Standalone
`/var/opt/drweb.com`	Bases de données virales, **Dr.Web Virus-Finding Engine**, fichiers temporaires et bibliothèques additionnelles requis pour le fonctionnement de **Dr.Web pour Linux**.

Supprimer Dr.Web pour Linux

En fonction de la méthode d'installation de **Dr.Web pour Linux**, pouvez supprimer la suite d'une des façons suivantes:

1. Démarrer le programme de désinstallation pour supprimer le package universel (pour les modes graphique ou en ligne de commande, en fonction de l'environnement).
2. Supprimer les packages installés depuis le dépôt de **Doctor Web** via le gestionnaire de packages système

Supprimer le Package Universel

Vous pouvez supprimer **Dr.Web pour Linux** installé grâce à la distribution du package universel pour les systèmes UNIX via le menu de l'application de l'environnement de bureau, ou via la ligne de commande.

Supprimer le logiciel via le menu de l'application

Dans le menu de l'application, cliquez sur l'onglet **Dr.Web et choisissez Supprimer les composants de Dr.Web**. L'Assistant de Suppression pour le mode graphique va s'ouvrir.

Supprimer le logiciel via la ligne de commande

Pour supprimer **Dr.Web pour Linux**, lancez le script **`remove.sh`** qui réside dans le répertoire `/opt/drweb.com/bin` en utilisant la commande suivante:

```
# /opt/drweb.com/bin/remove.sh
```

Puis un programme de désinstallation démarre (en mode graphique ou en ligne de commande selon l'environnement).

Pour lancer le programme de désinstallation directement depuis la ligne de commande, utilisez la commande suivante:

```
# /opt/drweb.com/bin/uninst.sh
```

La suppression de **Dr.Web pour Linux** est décrite dans les chapitres suivants :

- Suppression en Mode Graphique
- Suppression en Ligne de Commande

Suppression en Mode Graphique

Une fois que l'assistant de Suppression démarre en mode graphique, sa page de bienvenue où vous pouvez choisir la langue dans la liste déroulante dans le coin en haut à droite s'affiche.

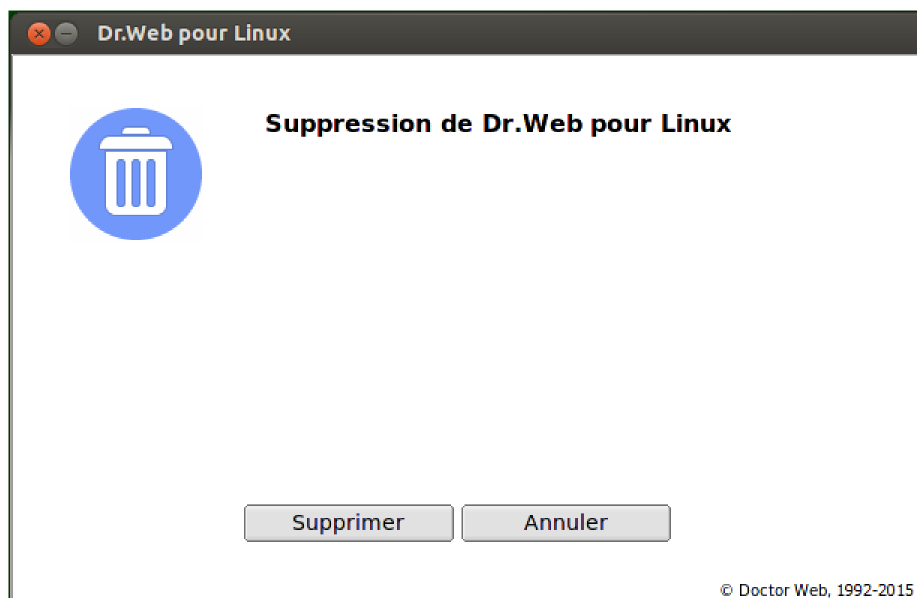


Image 14. Page de bienvenue

Pour désinstaller **Dr.Web pour Linux**, cliquez sur **Supprimer**. Pour fermer l'Assistant de Suppression, cliquez sur **Annuler**.

Après le démarrage de la suppression, une page avec une barre de progression s'ouvre. Si nécessaire, vous pouvez cliquer sur le bouton **Plus d'info** et voir les logs.



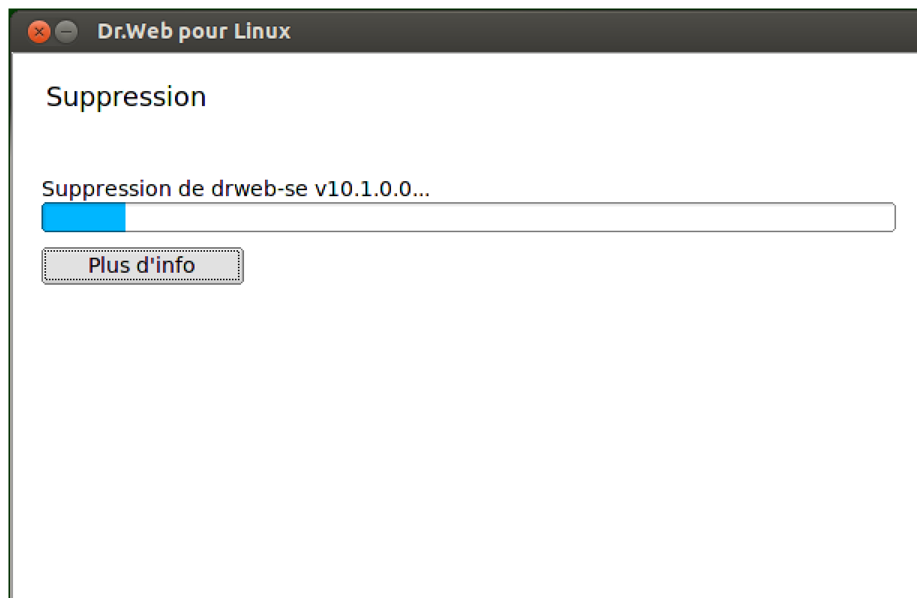


Image 15. Barre de progression de la suppression

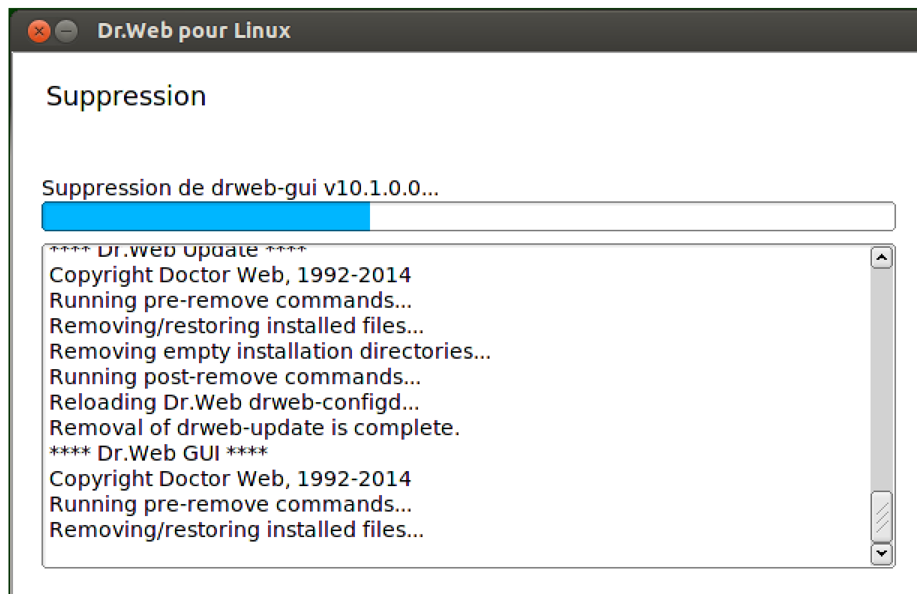


Image 16. Voir les logs

Une fois que les fichiers de **Dr.Web pour Linux** sont supprimés avec succès et que toutes les modifications nécessaires sont effectuées dans le système de fichiers, la dernière page de l'Assistant de Suppression s'affiche pour indiquer le succès de l'opération.



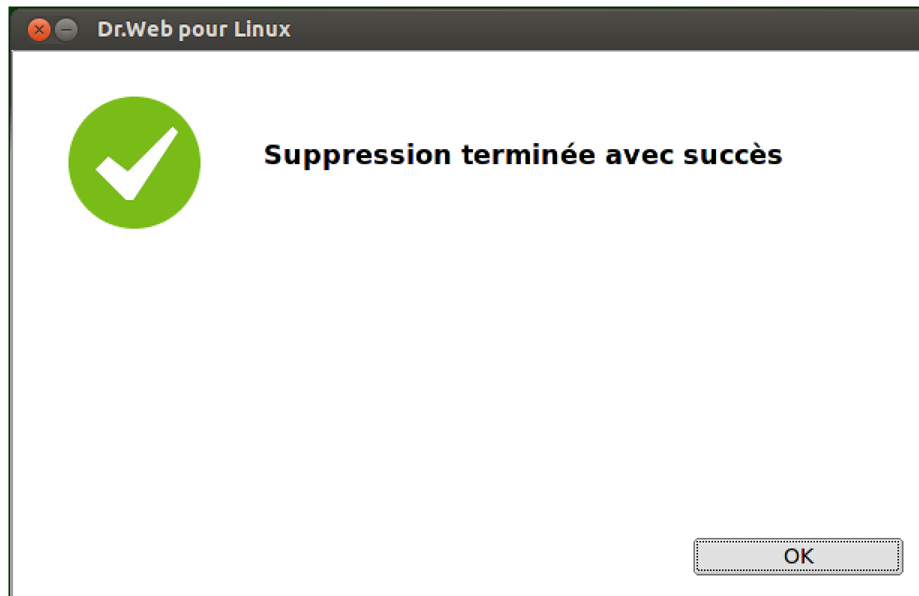


Image 17. Page de résultats de l'Assistant de Suppression

Pour fermer l'Assistant de Suppression, cliquez sur **OK**.

Supprimer en ligne de commande

Lorsque le programme de suppression pour le mode ligne de commande démarre, l'invite de commande s'affiche sur l'écran.

1. Pour démarrer la suppression, entrez **`Yes`** ou **`Y`** en réponse à la question "Souhaitez-vous continuer ?". Pour sortir du programme de suppression, tapez **`No`** ou **`N`**. Dans ce cas, la suppression sera annulée.

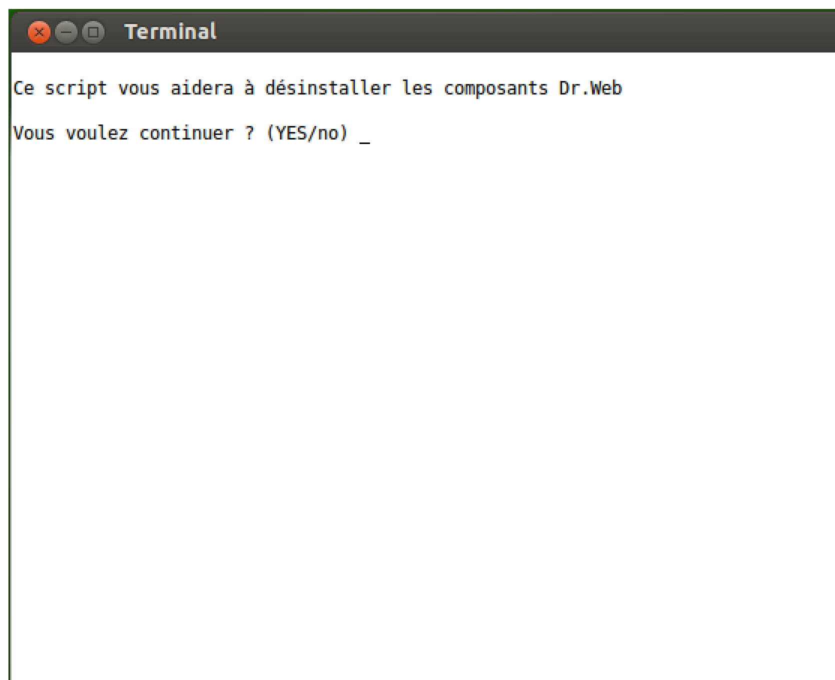


Image 18. Invite de commande pour désinstaller le produit

2. Après cela, une liste des composants **Dr.Web pour Linux** installés s'affiche.




```
        [ ] 8 Dr.Web Secutiry Suite agent (10.1.0.0)
        [ ] 9 Dr.Web Antivirus Filecheck backend (10.1.0.0)
        [ ] 10 Dr.Web Antivirus Firewall manager (10.1.0.0)
        [ ] 11 Dr.Web GateD (10.1.0.0)
        [ ] 12 Dr.Web GUI (10.1.0.0)
        [ ] 13 Essential third party libraries needed for Dr.Web on x86 systems
 (10.1.0.0)
        [ ] 14 Dr.Web Antivirus Netcheck backend (10.1.0.0)
        [ ] 15 OpenSSL - Secure Sockets Layer and cryptography shared libraries
 and tools (10.1.0.0)
        [ ] 16 Google protobuf needed for Dr.Web (10.1.0.0)
        [ ] 17 Qt, third party C++ libraries needed for Dr.Web (10.1.0.0)
        [ ] 18 Dr.Web Antivirus Daemon SE (10.1.0.0)
        [ ] 19 Dr.Web Spider Kernel Module (10.1.0.0)
        [ ] 20 Dr.Web Spider (10.1.0.0)
        [ ] 21 Dr.Web Update (10.1.0.0)
        [ ] 22 Dr.Web for Linux documentation (10.1.0.0)

Pour sélectionner un paquet à installer ou désélectionner
le paquet précédemment sélectionné, entrez le numéro du paquet et cliquez sur E
nter.

Entrez A ou All pour sélectionner tous les paquets, entrez N ou None pour
désélectionner tous les paquets.
Entrez R ou Remove pour supprimer les paquets sélectionnés.
Entrez 0, Q ou Quit pour quitter le programme d'installation.
Toutes les valeurs sont insensibles à la casse.
Sélectionner : _
```

Image 19. Voir la liste des composants installés

3. Pour continuer la suppression, sélectionnez les composants à supprimer. Pour sélectionner un composant en particulier, indiquez son numéro dans la liste. Notez que tous les packages dépendant d'un package sélectionné sont également automatiquement sélectionnés pour être supprimés.
   - Pour sélectionner tous les composants listés, tapez **`All`** ou **`A`** au lieu du numéro d'un composant
   - Pour rejeter la sélection des packages, tapez **`None`** ou **`N`** au lieu du numéro d'un composant.
   - Pour annuler la suppression, tapez **`0`**, **`Q`** ou **`Quit`** au lieu du numéro d'un composant. Si c'est le cas, le programme de suppression quitte.

```
        [X] 8 Dr.Web Secutiry Suite agent (10.1.0.0)
        [X] 9 Dr.Web Antivirus Filecheck backend (10.1.0.0)
        [X] 10 Dr.Web Antivirus Firewall manager (10.1.0.0)
        [X] 11 Dr.Web GateD (10.1.0.0)
        [X] 12 Dr.Web GUI (10.1.0.0)
        [X] 13 Essential third party libraries needed for Dr.Web on x86 systems
 (10.1.0.0)
        [X] 14 Dr.Web Antivirus Netcheck backend (10.1.0.0)
        [X] 15 OpenSSL - Secure Sockets Layer and cryptography shared libraries
 and tools (10.1.0.0)
        [X] 16 Google protobuf needed for Dr.Web (10.1.0.0)
        [X] 17 Qt, third party C++ libraries needed for Dr.Web (10.1.0.0)
        [X] 18 Dr.Web Antivirus Daemon SE (10.1.0.0)
        [X] 19 Dr.Web Spider Kernel Module (10.1.0.0)
        [X] 20 Dr.Web Spider (10.1.0.0)
        [X] 21 Dr.Web Update (10.1.0.0)
        [X] 22 Dr.Web for Linux documentation (10.1.0.0)

Pour sélectionner un paquet à installer ou désélectionner
le paquet précédemment sélectionné, entrez le numéro du paquet et cliquez sur E
nter.

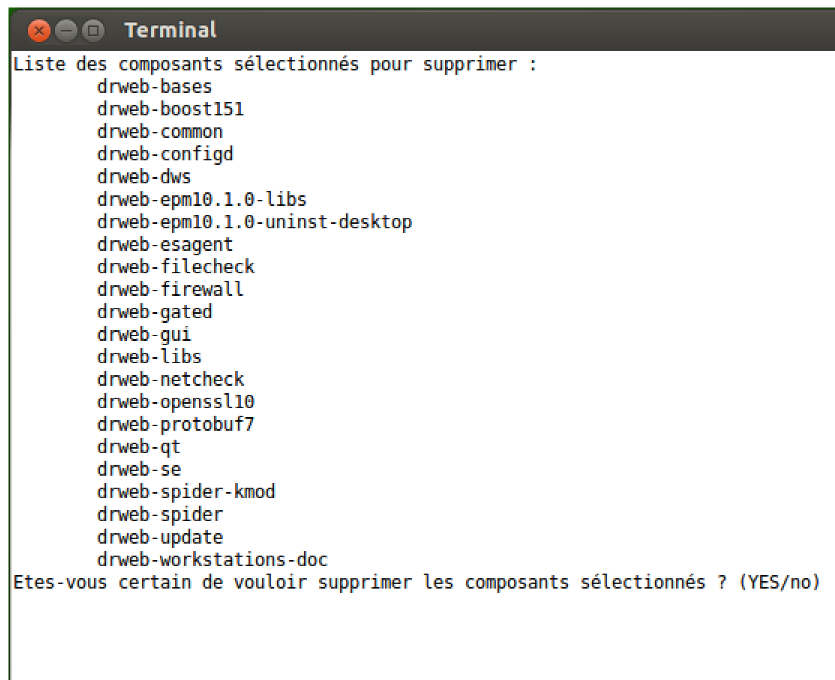
Entrez A ou All pour sélectionner tous les paquets, entrez N ou None pour
désélectionner tous les paquets.
Entrez R ou Remove pour supprimer les paquets sélectionnés.
Entrez 0, Q ou Quit pour quitter le programme d'installation.
Toutes les valeurs sont insensibles à la casse.
Sélectionner : _
```

Image 20. Sélection de composants à supprimer

4. Après avoir sélectionné les composants à supprimer, tapez **`Remove`** ou **`R`** pour démarrer le



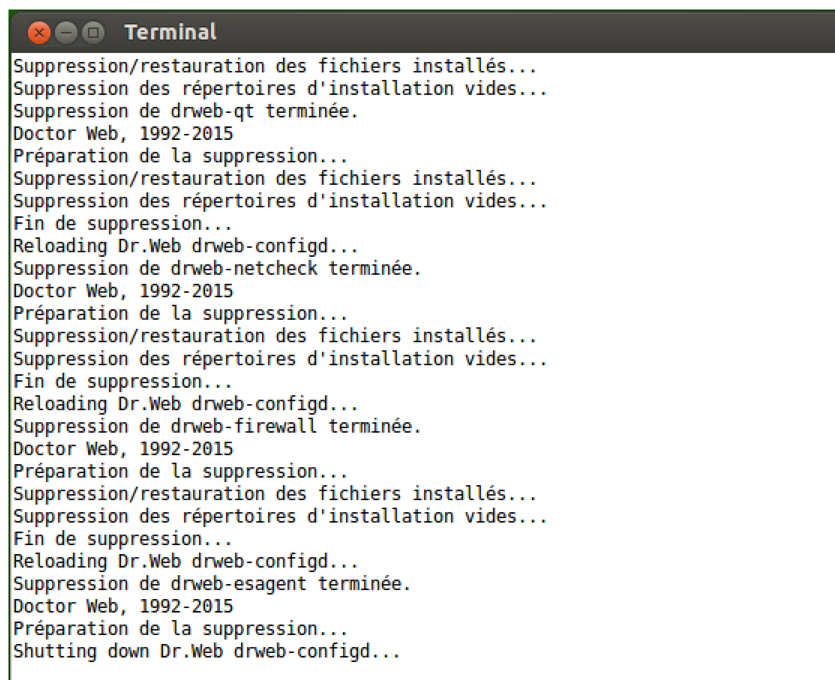
processus.



```
Liste des composants sélectionnés pour supprimer :
        drweb-bases
        drweb-boost151
        drweb-common
        drweb-configd
        drweb-dws
        drweb-epm10.1.0-libs
        drweb-epm10.1.0-uninst-desktop
        drweb-esagent
        drweb-filecheck
        drweb-firewall
        drweb-gated
        drweb-gui
        drweb-libs
        drweb-netcheck
        drweb-openssl10
        drweb-protobuf7
        drweb-qt
        drweb-se
        drweb-spider-kmod
        drweb-spider
        drweb-update
        drweb-workstations-doc
Etes-vous certain de vouloir supprimer les composants sélectionnés ? (YES/no)
```

Image 21. Confirmation de suppression d'un composant

5. Sur la page suivante, vous pouvez voir la liste des packages sélectionnés pour être supprimés et confirmer l'action en tapant `Yes` ou `Y.`. Si vous choisissez de ne pas supprimer les composants, quittez le programme de suppression en tapant `No` ou `N`.



```
Suppression/restauration des fichiers installés...
Suppression des répertoires d'installation vides...
Suppression de drweb-qt terminée.
Doctor Web, 1992-2015
Préparation de la suppression...
Suppression/restauration des fichiers installés...
Suppression des répertoires d'installation vides...
Fin de suppression...
Reloading Dr.Web drweb-configd...
Suppression de drweb-netcheck terminée.
Doctor Web, 1992-2015
Préparation de la suppression...
Suppression/restauration des fichiers installés...
Suppression des répertoires d'installation vides...
Fin de suppression...
Reloading Dr.Web drweb-configd...
Suppression de drweb-firewall terminée.
Doctor Web, 1992-2015
Préparation de la suppression...
Suppression/restauration des fichiers installés...
Suppression des répertoires d'installation vides...
Fin de suppression...
Reloading Dr.Web drweb-configd...
Suppression de drweb-esagent terminée.
Doctor Web, 1992-2015
Préparation de la suppression...
Shutting down Dr.Web drweb-configd...
_
```

Image 22. Log de désinstallation

6. Après le démarrage de la suppression des composants sélectionnés, des messages sur le processus de suppression s'affichent sur l'écran et sont journalisés.

```
Terminal
Doctor Web, 1992-2015
Removing/restoring installed files...
Removing empty installation directories...
Running post-remove commands...
Removal of drweb-epm10.1.0-uninst is complete.
Doctor Web, 1992-2015
Removing/restoring installed files...
Removing empty installation directories...
Removal of drweb-epm10.1.0-libs is complete.
Copyright Boost authors.
Removing/restoring installed files...
Removing empty installation directories...
Removal of drweb-boost151 is complete.
Doctor Web, 1992-2015
Removing/restoring installed files...
Removing empty installation directories...
Removal of drweb-libs is complete.
Doctor Web, 1992-2015
Removing/restoring installed files...
Removing empty installation directories...
Removal of drweb-common is complete.
root@userm:/opt/drweb.com# _
```

Image 23. Message de fin de désinstallation

7. Une fois la désinstallation terminée, le programme affiche un message correspondant et quitte.

Supprimer le Produit Installé depuis le Dépôt



Toutes les commandes mentionnées ci-dessous pour le package de suppression requièrent les privilèges administrateur (`root`). Pour élever les privilèges, utilisez la commande **`su`** (modifier l'utilisateur en cours) ou la commande **`sudo`** (exécuter la commande indiquée avec les privilèges d'un autre utilisateur).

Debian, Ubuntu (apt)

Pour supprimer le meta-package racine de **Dr.Web pour Linux**, entrez la commande suivante :

```
# apt-get remove drweb-workstations
```

Pour supprimer tous les packages de **Dr.Web** installés, entrez la commande suivante (dans certains systèmes d'exploitation, le symbole '`*`' doit être évité : '`\*`') :

```
# apt-get remove drweb*
```

Pour supprimer automatiquement tous les packages qui ne sont plus utilisés, entrez la commande suivante :

```
# apt-get autoremove
```



Veuillez noter quelques aspects spécifiques de la suppression avec la commande **`apt-get`** :

1. La première version mentionnée de la commande supprime uniquement le package `drweb-workstations` ; tous les autres packages qui pourraient être installés automatiquement pour résoudre les dépendances restent dans le système.
2. La seconde version mentionnée de la commande supprime tous les packages dont le nom commence par "`drweb`" (préfixe du nom standard pour les produits **Dr.Web**). Notez que cette commande supprime tous les packages portant ce préfixe, et non uniquement ceux de **Dr.Web pour Linux**.
3. La troisième version mentionnée de la commande supprime tous les packages qui ont été automatiquement installés pour résoudre les dépendances d'autres packages et ne sont plus nécessaires (par ex. à cause de leur suppression). Notez que cette commande supprime tous les packages qui ne sont pas utilisés, et non uniquement ceux de **Dr.Web pour Linux**.

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple, **Synaptic** ou **aptitude**)

pour supprimer les packages.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

Pour supprimer tous les packages installés de **Dr.Web**, entrez la commande suivante (dans certains systèmes d'exploitation, le symbole '*' doit être évité : '*') :

```
# yum remove drweb*
```



Veuillez noter quelques aspects spécifiques de la suppression avec la commande **yum** :

Cette version de la commande supprime tous les packages dont le nom commence par "drweb" (préfixe du nom standard pour les produits **Dr.Web**). Notez que cette commande supprime tous les packages portant ce préfixe, et non uniquement ceux de **Dr.Web pour Linux**.

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple **PackageKit** ou**Yumex**) pour supprimer les packages.



Travailler avec Dr.Web pour Linux

Vous pouvez travailler avec **Dr.Web pour Linux**

- Via l'interface graphique (dans un environnement de bureau graphique)
- Depuis la ligne de commande du système d'exploitation, y compris des simulateurs de terminal pour le mode graphique

Pour démarrer **Dr.Web pour Linux** en mode graphique, sélectionnez l'onglet **Dr.Web pour Linux** dans le menu ou entrez la commande suivante dans la ligne de commande du système d'exploitation

```
$ drweb-gui
```

Dans ce cas, si l'environnement de bureau est disponible, **Dr.Web pour Linux** démarre en mode graphique.

Pour en savoir plus sur la gestion du fonctionnement de **Dr.Web pour Linux**, référez-vous à la section Fonctionnement en ligne de commande.

Lorsque **Dr.Web pour Linux**fonctionne normalement, un indicateur d'état apparaît dans la zone de notifications (si l'environnement de bureau est disponible) et fournit l'accès au menu du logiciel ou affiche des notifications pop-up. L'indicateur, comme d'autres composants service, démarre automatiquement et son fonctionnement ne requiert pas l'intervention de l'utilisateur.



Quel que soit le mode d'installation de **Dr.Web pour Linux**, après la fin de l'installation, vous devez soit activer la licence, soit installer le fichier clé si vous l'avez déjà obtenu, ou connecter **Dr.Web pour Linux** au serveur de protection centralisée (voir Licencing).

Tant que vous n'aurez pas fait cela, **la protection antivirus sera désactivée.**

Fonctionnement en mode graphique

L'interface graphique de **Dr.Web pour Linux** est une application à base de fenêtres fonctionnant dans un environnement de bureau graphique et utilisée pour la gestion du fonctionnement de **Dr.Web pour Linux**.

Fonctions principales

L'interface graphique de **Dr.Web pour Linux** permet de

1. Voir le statut du fonctionnement de **Dr.Web pour Linux**, y compris le statut des bases virales et la durée de validité de la licence
2. Démarrer et arrêter **SpIDer Guard**
3. Démarrer et arrêter **SpIDer Gate**
4. Lancer un scan à la demande dans l'un des modes suivants :
   - **Scan rapide** pour vérifier les fichiers système et les objets systèmes les plus critiques
   - **Scan complet** pour vérifier tous les fichiers accessibles dans le système de fichiers
   - **Scan personnalisé** pour vérifier uniquement les fichiers et dossiers indiqués par l'utilisateur, ou des objets spécifiques (secteurs d'amorçage des disques, processus actifs)

   Vous pouvez également indiquer des fichiers à scanner en sélectionnant des fichiers et dossiers avant le démarrage du scan ou en les glissant/déposant de la fenêtre de gestion de fichier vers la page Principale (voir ci-dessous) ou Page de scan de la fenêtre de **Dr.Web pour Linux**.
5. Voir toutes les menaces détectées sur l'ordinateur par **Dr.Web pour Linux** durant son fonctionnement en mode graphique, y compris les menaces neutralisées et passées et les objets



placés en quarantaine.

6. Voir les objets placés en quarantaine, les supprimer ou les restaurer
7. Configurer les paramètres de **Dr.Web pour Linux** y compris :
   - Les actions à appliquer aux menaces détectées (en fonction de leur type) par le **Scanner** et **SpIDer Guard**
   - La liste des fichiers et dossiers qui ne devraient pas être analysés par le **Scanner** ou vérifiés par **SpIDer Guard**
   - Listes noires et blanches de sites web utilisées par **SpIDer Gate**, et paramètres de scan des fichiers téléchargés sur Internet
   - Planification des tâches de scan incluant la périodicité et le type de scan effectué, et la liste des objets à scanner
   - Mode de fonctionnement (statut de la connexion au serveur de protection centralisée)
   - Autorisation d'utiliser le service **Dr.Web Cloud**
8. Gestion de la licence (effectuée via le **Gestionnaire de Licences**).



Pour permettre un fonctionnement correct, assurez-vous que tous les composants service sont lancés avant le démarrage de **Dr.Web pour Linux** ; Sinon, il s'arrête immédiatement après le démarrage après avoir affiché une alerte correspondante.

Dans le cadre d'un fonctionnement normal, tous les composants requis sont démarrés automatiquement et ne nécessitent pas l'intervention de l'utilisateur.

Apparence

L' apparence de la page Principale de **Dr.Web pour Linux** est présentée dans l'image ci-dessous.

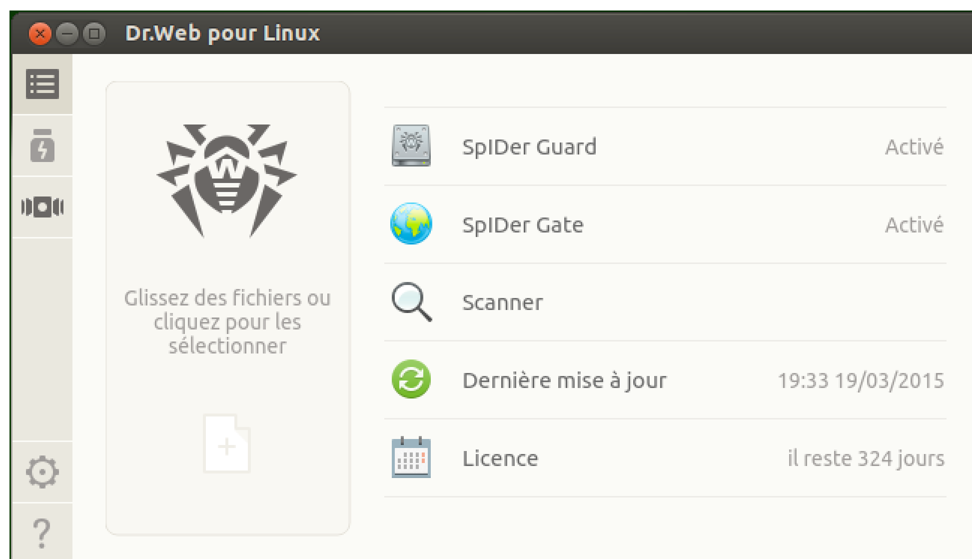


Image 24. Fenêtre principale de Dr.Web pour Linux

Le volet gauche de la fenêtre affiche les boutons de navigation qui permettent d'effectuer les actions suivantes.

Bouton	Description
Activé en continu	
	Ouvre la page Principale où vous pouvez • Activer ou désactiver **SpIDer Guard** • Activer ou désactiver **SpIDer Gate**



Bouton	Description
	• Lancer le scan des objets du système de fichiers (fichiers, secteurs d'amorçage) et des processus en cours • Voir le statut de la base virale et la mettre à jour si nécessaire • Lancer le **Gestionnaire de Licences** pour voir le statut de la licence en cours et enregistrer une nouvelle licence si nécessaire
	Ouvrir la page de la Quarantaine pour voir les fichiers placés en quarantaine, les supprimer ou les restaurer
	Ouvrir la fenêtre des paramètres de **Dr.Web pour Linux** incluant • Paramètres du **Scanner** • Paramètres de **SpIDer Guard** • Paramètres de **SpIDer Gate** • Lancer des scan sur planification De plus, sur cette page, vous pouvez configurer les paramètres du mode protection centralisée.
	Fournit un accès aux ressources de **Doctor Web** • Information produit • Manuel utilisateur • Forum officiel • Support technique • Page web personnelle de l'utilisateur **Mon Dr.Web.** Tous les liens ouvrent des pages web dans le navigateur installé sur votre ordinateur.
Visible sous certaines conditions	
	Ouvre la page avec la liste des tâches de scan incomplètes. Le bouton est visible sur le volet uniquement si au moins une tâche de scan est en cours.
	Ouvre la page avec les résultats des tâches de scan accomplies Le bouton change de couleur en fonction des résultats du scan 1) Vert – toutes les tâches de scan ont été accomplies avec succès ; Toutes les menaces détectées, s'il y en avait, ont été neutralisées 2) Rouge – certaines menaces détectées n'ont pas été neutralisées 3) Jaune – au minimum une des tâches de scan a échoué Le bouton est visible dans le volet uniquement si au moins un des tâches de scan a démarré.
	Ouvre la page sur laquelle les menaces détectées par le **Scanner** ou par **SpIDer Guard** sont listées. Le bouton est visible sur le volet si au moins une menace a été détectée.
	Le bouton est visible sur le volet uniquement si la page de lancement du scan est ouverte et active. Lors du passage à une autre page de la fenêtre principale ou lors du lancement du scan, la page de lancement du scan sera fermée automatiquement et le bouton sur le volet ne sera plus visible.
	Le bouton est visible sur le volet uniquement si au moins une page de gestion de **SpIDer Guard** est ouverte et active. Lors du passage à une autre page de la fenêtre principale, la page de gestion de **SpIDer Guard** sera fermée automatiquement et le bouton sur le volet ne sera plus visible.
	Le bouton est visible sur le volet uniquement si au moins une page de gestion de **SpIDer Gate** est ouverte et active. Lors du passage à une autre page de la fenêtre principale, la page de gestion de **SpIDer Gate** sera fermée automatiquement et le bouton sur le volet ne sera plus visible.



Bouton	Description
	Le bouton est visible sur le volet uniquement si au moins une page de gestion des mises à jour est ouverte et active. Lors du passage à une autre page de la fenêtre principale, la page de gestion des mises à jour sera fermée automatiquement et le bouton sur le volet ne sera plus visible.
	Le bouton est visible sur le volet uniquement si au moins une page de gestion du **Gestionnaire de licence** est ouverte et active. Lors du passage à une autre page de la fenêtre principale, la page de gestion du **Gestionnaire de licence** sera fermée automatiquement et le bouton sur le volet ne sera plus visible.

Page Principale

Sur la page Principale vous pouvez trouver le volet où vous pouvez glisser/déposer des fichiers et dossiers à scanner. Sur le volet apparaît la mention **Glissez des fichiers ou cliquez pour les sélectionner**. Une fois les objets glissés/déposés depuis le gestionnaire de fichiers vers la page Principale, leur scan démarre (si le **Scanner** scanne déjà d'autres objets, la nouvelle tâche de scan est mise en file d'attente).

Sur cette page, les boutons suivants sont disponibles :

- **SpIDer Guard** – affiche le statut en cours de **SpIDer Guard**. Cliquez sur ce bouton pour ouvrir la page de **SpIDer Guard** donnant accès aux paramètres du composant et sur laquelle vous pouvez lancer ou arrêter **SpIDer Guard** ainsi que consulter les statistiques sur son fonctionnement.
- **SpIDer Gate** – affiche le statut en cours de **SpIDer Gate**, qui gère l'accès aux ressources web. Cliquez sur ce bouton pour ouvrir la page de gestion, sur laquelle vous pouvez lancer ou arrêter **SpIDer Gate** et consulter les statistiques sur son fonctionnement.
- **Scanner** – permet d'ouvrir la page sur laquelle vous pouvez lancer le scan de fichiers et autres objets système (par exemple, les secteurs d'amorçage).
- **Dernière mise à jour** – affiche le statut en cours des bases virales Cliquez sur ce bouton pour ouvrir la page indiquant le statut de la mise à jour et sur laquelle vous pouvez lancer une mise à jour si nécessaire.
- **Licence** – affiche le statut de la licence en cours. Cliquez sur ce bouton pour ouvrir la page du **Gestionnaire de Licences** sur laquelle vous pouvez trouver des informations détaillées sur la licence en cours ainsi qu'acheter et enregistrer une nouvelle licence si nécessaire.

Démarrer et arrêter l'interface graphique

Démarrer Dr.Web pour Linux en mode graphique

Pour démarrer **Dr.Web pour Linux** en mode graphique, faites une des actions suivantes :

- Sélectionnez l'onglet **Dr.Web pour Linux** dans le **Menu des Applications**.
- Cliquez droit sur l'icône de l'indicateur de **Dr.Web pour Linux** dans la zone de notification et choisissez **Ouvrir Dr.Web pour Linux**.

Vous pouvez également démarrer **Dr.Web pour Linux** en mode graphique depuis la ligne de commande. Vous pouvez utiliser cette option uniquement si l'environnement graphique est accessible en mode ligne de commande, par exemple, en travaillant sur une fenêtre de terminal.

Arrêter Dr.Web pour Linux

Pour arrêter **Dr.Web pour Linux**, fermez la fenêtre via le bouton classique fermer sur la barre de titre.





Notez que les composants service, y compris l'indicateur d'état, **SpIDer Guard** et **SpIDer Gate**, continuent à fonctionner après l'arrêt de l'interface graphique de **Dr.Web pour Linux** (à moins qu'ils ne soient stoppés par l'utilisateur).

Dans un fonctionnement normal, le fonctionnement des composants service ne requiert pas l'intervention de l'utilisateur.

Indicateur d'Etat dans la Zone de Notifications

Après la connexion de l'utilisateur, un indicateur d'état apparaît dans la zone de notifications comme icône de **Dr.Web pour Linux** (si cela est supporté par l'environnement graphique utilisé). L'indicateur affiche l'état du logiciel et fournit un accès au menu de **Dr.Web pour Linux**. Si un problème survient (les bases virales ne sont pas à jour ou la licence est sur le point d''expirer), l'indicateur affiche une icône avec un point d'exclamation : .

L'indicateur est utilisé pour afficher des notifications pop-up qui informent l'utilisateur des événements importants dans le fonctionnement de **Dr.Web pour Linux** comme :

- Les menaces détectées (y compris celles détectées par **SpIDer Guard** et **SpIDer Gate**)
- La durée de validité de la licence est sur le point d'expirer

Lorsque l'on clique sur l'icône, le menu de **Dr.Web pour Linux** s'affiche sur l'écran.

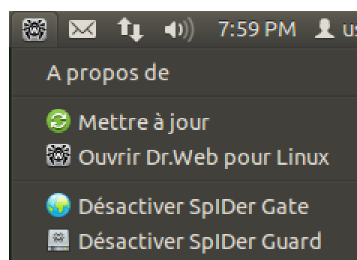


Image 25. Dr.Web pour Linux menu

Lorsque vous choisissez l'onglet **Ouvrir Dr.Web pour Linux**, la fenêtre principale de **Dr.Web pour Linux** apparaît sur l'écran ; le fonctionnement de **l'Antivirus** passe en mode graphique. La sélection des onglets **Activer/Désactiver SpIDer Gate** ou **SpIDer Guard** démarre ou arrête les moniteurs correspondants. Notez que vous devez vous authentifier en tant qu'utilisateur ayant les privilèges administrateur pour désactiver tout moniteur (consultez la section Privilèges de Gestion des Applications). La sélection de l'onglet **Mettre à jour** lance une procédure de mise à jour.

Si l'indicateur signale un problème dans le fonctionnement de **Dr.Web pour Linux**, l'icône du composant qui a provoqué le problème s'affiche avec un point d'exclamation, par exemple : .

Problèmes de l'Indicateur d'etat

Si l'indicateur affiche la marque d'une erreur critique , et que le menu déroulant ne contient qu'un seul sujet affiché **Chargement...**, cela signifie que **Dr.Web pour Linux** ne peut pas démarrer parce que certains composants du noyau ne sont pas disponibles. Si cet état est permanent, essayez de résoudre l'erreur manuellement ou contactez le Support technique.

Si après la connexion de l'utilisateur au système, l'indicateur n'a pas été affiché dans la zone de notifications du bureau, essayez de résoudre cette erreur ou contactez le Support technique.





Selon l'environnement de bureau, l'apparence et le comportement de l'indicateur peuvent être différents de celui décrit plus haut ; Par exemple, les icônes peuvent ne pas s'afficher dans le menu déroulant.

Détection et neutralisation des menaces

La recherche et la neutralisation des menaces peuvent être lancées soit par le **Scanner** à la demande de l'utilisateur, ou selon la planification, ou par **SpIDer Guard**.

- Pour activer ou désactiver **SpIDer Guard** et **SpIDer Gate**, utilisez le menu contextuel dans la zone de notifications ou ouvrez la page correspondante des paramètres du moniteur (consultez les sections Gérer le Système de Fichiers et Gérer l'Accès Internet).
- Pour voir les tâches en cours du **Scanner** ou les gérer, ouvrez la page de gestion des tâches.
- Pour voir les menaces détectées par le **Scanner** ou durant les contrôles de **SpIDer Guard**, ouvrez la page les menaces listées.
- Pour gérer les menaces placées en quarantaine, ouvrez la page de la Quarantaine.
- Pour configurer les réactions de **Dr.Web pour Linux** face aux menaces détectées, ouvrez la la fenêtre des paramètres. Sur cette page, vous pouvez également définir une planification pour lancer le scan.



Veuillez noter que si **Dr.Web pour Linux** opère en mode protection centralisée et que le lancement du scan à la demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, la page de lancement du scan et bouton **Scanner** de la fenêtre de **Dr.Web pour Linux** sera désactivée. De plus, dans ce cas, le **Scanner** ne lancera pas de scan même s'ils sont planifiés.

Scan à la demande

Types de scan

À la demande de l'utilisateur, le scan dans un des modes suivants peut être lancé :

- *Scan rapide* – scan des objets systèmes critiques exposés à un fort risque de compromission (secteurs d'amorçage, système de fichiers, etc.)
- *Scan complet* – scan de tous les objets du système de fichiers accessibles à l'utilisateur sous le compte duquel a été lancé **Dr.Web pour Linux**
- *Scan personnalisé* – scan des objets du système de fichiers ou d'autres objets spécifiques indiqués par l'utilisateur.



Si **Dr.Web pour Linux** fonctionne en mode Protection centralisée et que le lancement d'un scan à la demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, la page est désactivée.

Le scan peut augmenter la charge du processeur, ce qui peut provoquer un déchargement rapide de la batterie. Ainsi, il est recommandé d'effectuer le scan d'un ordinateur portable lorsqu'il est branché.

Démarrer le scan

Pour démarrer le scan, cliquez sur le bouton **Scanner** sur la Page principale.

La page avec les différents types de scan s'ouvre Pour démarrer un scan *Rapide* ou *Complet*, cliquez sur le bouton correspondant. Après avoir cliqué sur l'un de ces boutons, le scan démarre automatiquement.





Image 26. Choisir la page de type de scan



Le scan est effectué avec les privilèges actuels du logiciel. Si l'utilisateur dont les privilèges sont actuellement actifs ne possède pas de permissions de superuser, tous les fichiers et répertoires qui ne lui sont pas accessibles ne peuvent pas être scannés. Pour permettre le scan de tous les fichiers souhaités sur lesquels vous n'avez pas de permissions de propriétaire, élevez les privilèges du logiciel avant le démarrage du scan. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.

Pour démarrer un *scan Personnalisé* de certains fichiers et répertoires, faites une des actions suivantes :

- **Glissez/déposez les objets souhaités**

  Glissez/déposez les fichiers et répertoires souhaités depuis la fenêtre du Gestionnaire du système de fichiers vers la zone portant la mention **Glissez des fichiers ou cliquez pour les sélectionner**. Vous pouvez également glisser/déposer les objets vers la Page principale.

  Lorsque vous glissez des objets sur la page, elle se modifie pour afficher le message **Déposez les fichiers ici** pour démarrer le scan, déposez les objets glissés dans la zone appropriée



Image 27. Zone où les objets sont glissés pour être scannés

- **Liste les objets à scanner.**



Pour sélectionner les objets à scanner, cliquez sur la zone dédiée La fenêtre dans laquelle vous pouvez sélectionner les objets système pour un scan Personnalisé s'ouvre.

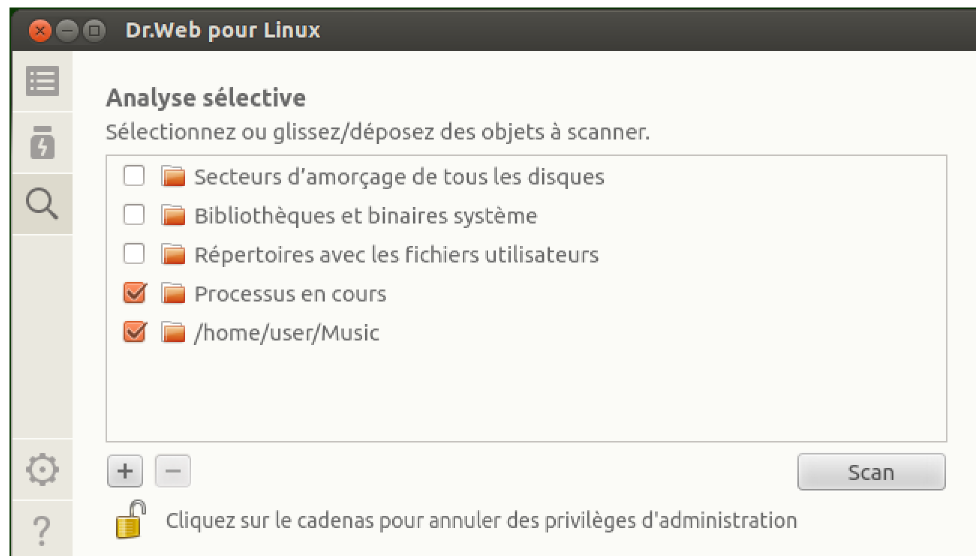


Image 28. Liste des objets à scanner

La liste des objets pour un scan Personnalisé contient quatre parties prédéfinies :

- *Secteurs d'amorçage de tous les disques.* Si vous cochez cette case, tous les secteurs d'amorçage de tous les disques disponibles sont sélectionnés pour être scannés. .
- *Bibliothèques et binaires système.* Si vous cochez cette case, tous les répertoires avec des systèmes binaires sont sélectionnés pour être scannés (`/bin`, `/sbin`, etc.);
- *Répertoires avec les fichiers utilisateurs.* Si vous cochez cette case, tous les répertoires contenant des fichiers utilisateurs et les fichiers de la session en cours sont sélectionnés pour être scannés (`/home/<username> (~)`, `/tmp`, `/var/mail`, `/var/tmp`).
- *Processus en cours.* Si vous cochez cette case, les fichiers exécutables binaires contenant le code des processus en cours sont sélectionnés pour être scannés. Dans ce cas, si une menace est détectée, non seulement l'objet malveillant est neutralisé, mais le processus actif est également arrêté.

Modifier la liste des objets de scan Personnalisé

Si nécessaire, vous pouvez ajouter des chemins personnalisés vers une liste d'objets à scanner. Pour cela, glissez/déposez les objets souhaités (les chemins vers les objets sont automatiquement ajoutés à la liste) ou cliquez sur le bouton « + » sous la liste. Dans ce cas, une fenêtre de dialogue standard s'ouvre où vous pouvez sélectionner les objets (un fichier ou un répertoire). Après avoir sélectionné les objets, cliquez sur **Ouvrir.** Pour supprimer tous les chemins sélectionnés de la liste, cliquez sur le bouton « – ».



Les fichiers et répertoires masqués ne sont pas affichés dans le sélecteur de fichiers par défaut. Pour voir ces objets, cliquez droit sur la liste de fichiers dans le sélecteur de fichiers et choisissez **Voir les fichiers masqués.**

Les quatre premières parties dans la liste sont prédéterminées et ne peuvent pas être supprimées même si les cases correspondantes sont cochées. De plus, si au moins une des parties prédéterminées est choisie, le bouton « – » est indisponible.

Lancer le scan Personnalisé des objets listés

Pour lancer le scan Personnalisé des objets listés, sélectionnez tous les fichiers ou répertoires requis et cliquez sur **Scan.** Après quoi le scan des objets démarre.



Après le démarrage du scan, la tâche est mise en file d'attente, qui contient toutes les tâches de scan de la session en cours : tâches terminées, tâches en cours, tâches en attente. Vous pouvez voir la liste des tâches et les gérer sur la page de gestion des tâches de scan.

Gérer les tâches de scan

Vous pouvez voir la liste des tâches créées et des tâches en cours sur une page spécifique de **Dr.Web pour Linux**. Si au moins une tâche est en attente, un bouton qui ouvre la page de la liste des tâches devient visible sur le panneau de navigation. En fonction du statut des tâches en attente, le bouton présente les icônes suivantes :

	Au moins une des tâches n'est pas terminée (l'icône est animée).
	Toutes les tâches de scan dans la liste sont terminées ou arrêtées par l'utilisateur ; aucune menace n'a été détectée ou toutes les menaces détectées ont été neutralisées avec succès.
	Toutes les tâches de scan dans la liste sont terminées ou arrêtées par l'utilisateur ; certaines des menaces détectées n'ont pas été neutralisées.
	Toutes les tâches de scan dans la liste sont terminées ou arrêtées par l'utilisateur. Certaines tâches ont échoué.

Les tâches sont triées par date (depuis la première créée à la plus récente).

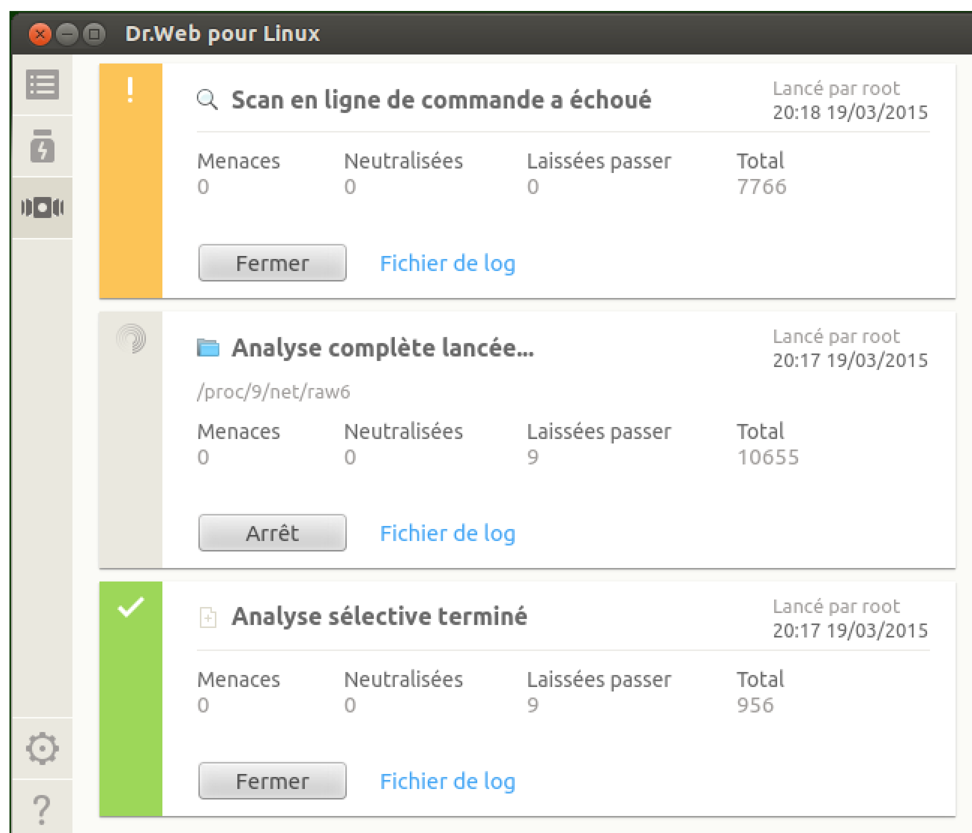


Image 29. Page de gestion des tâches

Pour chaque tâche listée, les informations suivantes sont disponibles :



- Type de scan (*Scan rapide, scan Complet et scan Personnalisé*, ou autres types de scan; pour en savoir plus, voir ci-dessous);
- Nom de l'utilisateur qui a lancé le scan (s'il est inconnu, l'UID du système s'affiche);
- Date de la création et de la fin de la tâche (si elle est terminée);
- Nombre de menaces détectées, menaces neutralisées, fichiers passés et nombre total d'objets scannés.

Le statut de la tâche est indiqué grâce à la couleur assignée à la tâche dans la liste. Les couleurs suivantes sont utilisées :

– Le scan n'est pas terminé ou est en attente.

– Le scan est terminé ou arrêté par l'utilisateur ; Aucune menace n'a été détectée ou toutes les menaces ont été neutralisées.

– Le scan s'est arrêté à cause d'une erreur.

– Le scan est terminé ou arrêté par l'utilisateur ; Au moins une des menaces détectées n'a pas été neutralisée.

Notez que la liste contient les tâches de scan effectuées par le **Scanner** durant la sessions en cours, et non uniquement les tâches créées par l'utilisateur en mode graphique. Les autres types de scan peuvent être les suivants :

- *Scan via la console* - Scan initié par l'utilisateur ou une application extérieure via l'interface de la ligne de commande;
- *Scan centralisé* - Scan initié par le serveur de protection centralisée;
- *Scan planifié* - Scan lancé automatiquement d'après la planification.

Dans la zone de description de la tâche, l'un des boutons suivants est disponible:

- **Annuler** – Annule la tâche en attente. Le bouton est disponible si la tâche est en attente. Après avoir cliqué dessus, la tâche se termine. L'information sur la tâche demeure dans la liste.
- **Stopper** – Stoppe la tâche en cours. Après avoir cliqué sur ce bouton, la tâche stoppée ne peut pas être relancée. Le bouton est disponible si la tâche est en cours. L'information sur la tâche stoppée demeure dans la liste.
- **Fermer** – Ferme les données sur la tâche terminée et supprime la tâche de la liste. Le bouton est disponible si la tâche n'est pas terminée et si toutes les menaces détectées ont été neutralisées.
- **Neutraliser** – Neutralise les menaces. Le bouton est disponible si la tâche est terminée et que certaines menaces n'ont pas été neutralisées.
- **Détails** - Ouvre la liste des menaces détectées et les neutralise. Le bouton est disponible si la tâche est terminée et que certaines menaces n'ont pas été neutralisées.

Cliquez sur **Journal** pour afficher les résultats du scan incluant des données détaillées sur la tâche et la liste des menaces détectées, s'il y en a.



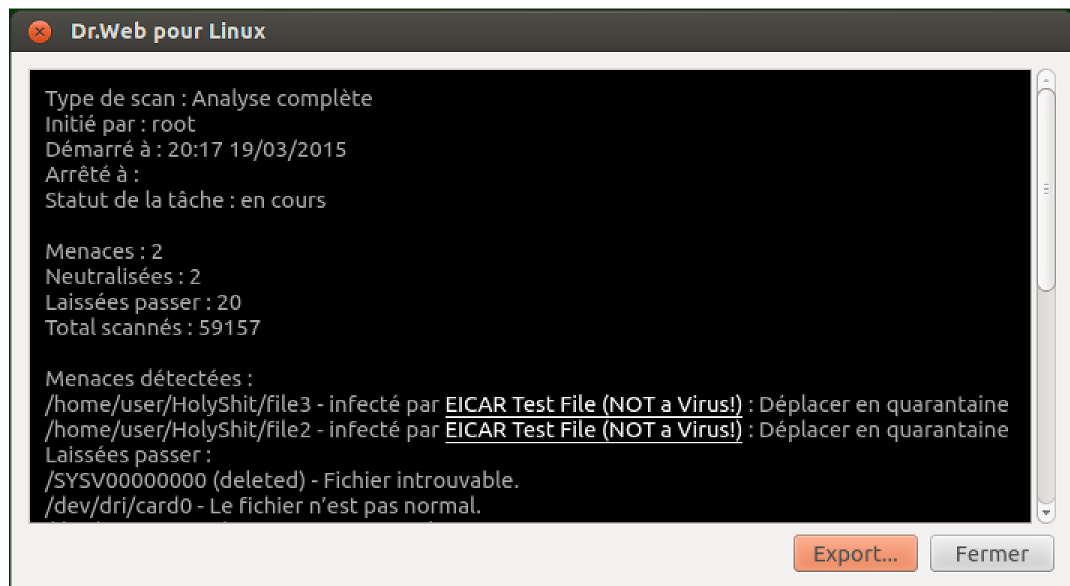


Image 30. Information détaillée sur les résultats du scan

Notez que: Les systèmes de fichiers UNIX, tels que **Linux,** peuvent contenir des objets spéciaux qui apparaissent comme des noms de fichiers mais ne sont pas des fichiers contenant des données (ce sont, par exemple, des liens symboliques, des sockets, des canaux nommés et des fichiers de périphérique). Ils sont appelés fichiers *spéciaux*, à la différence des fichiers usuels (*réguliers*). **Dr.Web pour Linux** passe toujours les fichiers spéciaux durant le scan.

Cliquez sur **Exporter...** pour sauvegarder les données de scan vers un fichier texte. Cliquez sur le nom d'une menace détectée pour ouvrir, dans votre navigateur, une page web donnant des informations sur la menace (le nom de la menace est un lien vers le site officiel de **Doctor Web** ; Une connexion Internet valide est requise).

Pour chaque menace détectée durant le scan lancé en mode graphique (y compris un scan planifié), **Dr.Web pour Linux** applique des actions définies dans les paramètres à l'onglet **Scanner**.



Notez que les paramètres de neutralisation des menaces définis à l'onglet **Scanner** ne sont pas utilisés pour les scan *centralisé* et *via la console*.

Pour voir toutes les menaces détectées, ouvrez la page avec la liste des menaces détectées.

Gérer le Système de Fichiers

SpIDer Guard est un moniteur antivirus qui contrôle tous les objets du système de fichiers créés et modifiés.

Dans la fenêtre principale de **Dr.Web pour Linux** vous pouvez gérer **SpIDer Guard**

- Lancer et arrêter le contrôle du système de fichiers.
- Voir les statistiques sur le fonctionnement du composant et la liste des menaces détectées.
- Configurer les paramètres suivants:
  - Réactions face aux menaces détectées
  - Liste des exclusions

Gestion du fonctionnement

Vous pouvez lancer ou arrêter **SpIDer Guard**, ainsi que consulter ses statistiques sur une page spécifique.



Pour ouvrir la page, cliquez sur **SpIDer Guard** sur la page Principale.



Image 31. Page de gestion de SpIDer Guard

Sur la page des paramètres du moniteur, les informations suivantes sont fournies :

- Statut de **SpIDer Guard** et données sur les erreurs de démarrage (s'il y en a)
- Statistiques sur le fonctionnement de **SpIDer Guard** (nombre d'objets vérifiés, nombre de menaces détectées, nombre de menaces neutralisées)

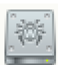
Pour activer le contrôle du système de fichiers, cliquez sur **Activer**. Pour désactiver le contrôle, cliquez sur **Désactiver.**



Pour désactiver le contrôle du système de fichiers, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.

Si **Dr.Web pour Linux** opère en mode Protection centralisée, l'option activer/désactiver **SpIDer Guard** peut être bloquée par l'administrateur et devenir indisponible.

Le statut du moniteur du système de fichiers **SpIDer Guard** (activé ou désactivé) est indiqué par l'une des icônes suivantes :

 – **SpIDer Guard** est activé et protège le système de fichiers.

 – **SpIDer Guard** a été désactivé par l'utilisateur ou stoppé à cause d'une erreur et ne protège pas le système de fichiers.

Pour fermer la page des paramètres de **SpIDer Guard**, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.

La liste des menaces détectées par **SpIDer Guard** durant la session en cours du GUI de **Dr.Web pour Linux** s'affiche sur la page des menaces listées (la page est disponible seulement si au moins une menace a été détectée).

Configurer SpIDer Guard

Pour configurer les paramètres de **SpIDer Guard**, ouvrez la page des Paramètres et cliquez sur

- L'onglet **SpIDer Guard** pour définir les réactions face aux menaces détectées



* L'onglet **Exclusions** pour lister les objets à exclure du contrôle du système de fichiers.

Problèmes de SpIDer Guard

Si un échec de **SpIDer Guard** est détecté, les informations sur l'erreur survenue s'affichent sur la page de gestion. Pour résoudre le problème, consultez l'Annexe D, où vous pouvez trouver une description détaillée des erreurs connues.

Gérer l'accès Internet

SpIDer Gate effectue un contrôle permanent de l'accès Internet. Le moniteur empêche l'accès aux sites web placés en liste noire et vérifie les fichiers téléchargés contre les virus et autres menaces.

La fenêtre de **Dr.Web pour Linux** permet de gérer **SpIDer Gate**, à savoir :

* Lancer et arrêter le moniteur
* Voir le nombre des objets vérifiés et bloqués et des tentatives d'accès aux sites
* Configurer les paramètres de surveillance Internet suivants :
  * Catégories de ressources web auxquelles l'accès est bloqué
  * Listes noire et blanche de ressources web de l'utilisateur
  * Paramètres de scan des fichiers téléchargés sur Internet.

Gérer SpIDer Gate

Vous pouvez lancer et arrêter **SpIDer Gate** ainsi que consulter ses statistiques sur une page spécifique dans la fenêtre de **Dr.Web pour Linux**. Pour l'ouvrir, vous pouvez soit cliquer sur **SpIDer Gate** sur la page Principale.



Image 32. Page de gestion de SpIDer Gate

Sur la page des paramètres du moniteur, les informations suivantes sont fournies :

* Statut de **SpIDer Gate** (activé ou désactivé), et données sur les erreurs de démarrage (s'il y en a)
* Statistiques sur la surveillance du web (nombre d'URL et d'objets téléchargés de l'Internet vérifiés, nombre de tentatives d'accès aux sites et d'objets contenant des menaces bloqués)

Pour démarrer le contrôle de l'accès Internet, cliquez sur **Activer**. Pour arrêter le contrôle de l'accès Internet, cliquez sur **Désactiver.**



Pour désactiver le contrôle du web, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.

Si **Dr.Web pour Linux** opère en mode Protection centralisée, l'option activer/désactiver **SpIDer Gate** peut être bloquée par l'administrateur et devenir indisponible.

Le statut du moniteur web **SpIDer Gate** (activé ou désactivé) est indiqué par l'une des icônes suivantes :



– **SpIDer Gate** est activé et contrôle l'accès aux ressources Internet.



– **SpIDer Gate** a été désactivé par l'utilisateur ou stoppé à cause d'une erreur et ne contrôle pas l'accès aux ressources Internet (l'accès aux sites web n'est pas restreint et le téléchargement de fichiers n'est pas contrôlé).

Pour fermer la page des paramètres de **SpIDer Gate**, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.

Configurer SpIDer Gate

Pour configurer les paramètres de **SpIDer Gate**, ouvrez la Page des paramètres et l'onglet **SpIDer Gate**.

Problèmes de SpIDer Gate

Si un échec de **SpIDer Gate** est détecté, les informations sur l'erreur survenue s'affichent sur la page de gestion. Pour résoudre le problème, consultez l'Annexe D, où vous pouvez trouver une description détaillée des erreurs connues.

Voir les Menaces Détectées

La liste des menaces détectées par le **Scanner** et par **SpIDer Guard** durant la session en cours de **Dr.Web pour Linux** s'affiche sur une page spéciale disponible seulement si au moins une menace a été détectée.

Si des menaces sont détectées, vous pouvez ouvrir cette page en cliquant sur le bouton correspondant sur le panneau de navigation du GUI.



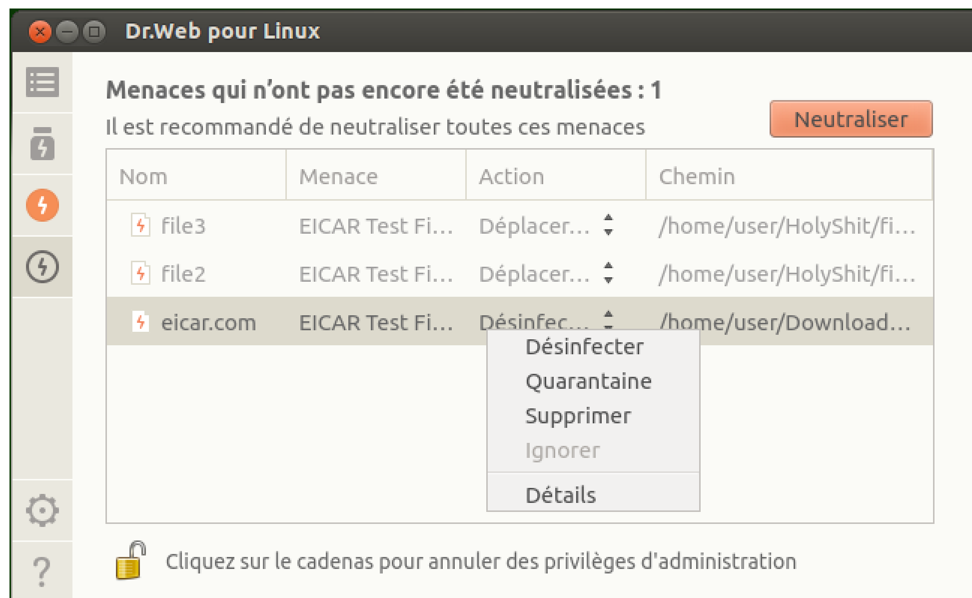


Image 33. Page des menaces listées

Dans la liste, les informations suivantes sont disponibles pour chaque menace détectée :

- Nom de l'objet malveillant
- Nom de la menace (d'après la classification de **Doctor Web)**
- Action appliquée (ou à appliquer) à la menace
- Chemin vers l'objet malveillant

Les menaces neutralisées s'affichent en grisé dans la liste.

Neutraliser les menaces détectées

Si certaines des menaces listées ne sont pas neutralisées, le bouton **Neutraliser** au-dessus de la liste devient disponible. Après avoir cliqué sur le bouton, les actions définies dans le champ **Action** correspondant sont appliquées aux menaces. Si une tentative de neutralisation d'une menace échoue, elle s'affiche en rouge et un message d'erreur apparaît dans le champ **Action**.

Par défaut, une action à appliquer à une menace est choisie d'après les paramètres du composant qui a détecté la menace. Vous pouvez configurer les actions appliquées aux menaces d'un certain type par le **Scanner** et par **SpIDer Guard**. Pour cela, ouvrez l'onglet correspondant sur la Page des paramètres et définissez les paramètres.

S'il est nécessaire d'appliquer une action différente de celle définie dans les paramètres, cliquez sur le champ **Action** et sélectionnez une action dans le menu.

Vous pouvez choisir plusieurs menaces en même temps dans la liste. Pour cela, sélectionnez les menaces avec la souris tout en maintenant appuyées les touches CTRL ou SHIFT.

- Lorsque vous maintenez appuyée la touché CTRL, les menaces sont sélectionnées une par une.
- Lorsque vous maintenez appuyée la touché SHIFT, les menaces sont sélectionnées toutes en même temps.

Après avoir sélectionné des menaces, vous pouvez leur appliquer l'action requise en cliquant droit sur la sélection puis en cliquant sur l'action dans le menu qui s'est affiché. L'action sélectionnée dans le menu est appliquée à toutes les menaces sélectionnées.





Notez que

- Si une menace est détectée dans un objet complexe (archive, email, etc), l'action sélectionnée est appliquée au conteneur comme un tout (et non uniquement à l'objet infecté);
- L'action **Réparer** ne peut être appliquée à tous les types de menaces.

Si nécessaire, élevez les privilèges du logiciel pour permettre une neutralisation réussie des menaces.

Voir les données sur les menaces

Pour des informations détaillées sur une menace, cliquez droit sur l'article avec les données sur la menace puis cliquez sur **Détails** dans le menu qui s'est affiché. Ensuite, une fenêtre s'ouvre contenant des informations détaillées sur la menace et les objets qui contenaient la menace. Pour consulter les données sur plusieurs menaces en même temps, sélectionnez les articles correspondants avec la souris tout en maintenant appuyée la touche CTRL.

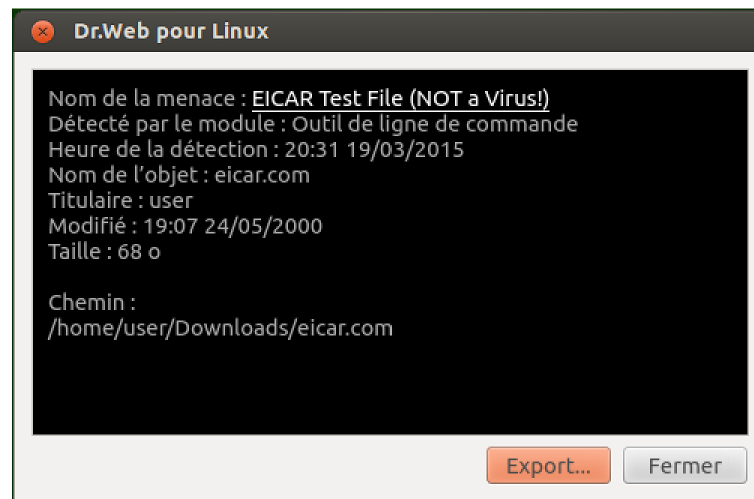


Image 34. Données sur une menace

Dans cette fenêtre, les informations suivantes sont fournies :

- Nom de la menace (d'après la classification de **Doctor Web**)
- Nom du composant **Dr.Web pour Linux** qui a détecté la menace
- Date et heure de la détection
- Information sur l'objet du système de fichiers dans lequel la menace a été détectée : nom de l'objet, propriétaire, date de la dernière modification et chemin vers l'objet dans le système de fichiers
- Dernière action appliquée à la menace et résultat (si l'option permettant d'appliquer des actions automatiquement à une menace est activée pour le composant)

Cliquer sur le lien du nom de la menace ouvre une page web avec des données sur la menace dans votre navigateur (le nom d'une menace est un lien vers le site officiel de **Doctor Web** ; une connexion Internet valide est requise). Vous pouvez également sauvegarder l'information affichée en cliquant sur **Exporter** (lorsque vous cliquez sur le bouton, une fenêtre où vous pouvez sélectionner un fichier pour la sauvegarde s'ouvre).

Pour fermer la fenêtre de données sur une menace ou un objet infecté, cliquez sur **Fermer**.

Gérer la quarantaine

La liste de fichiers déplacés en quarantaine par les composants de **Dr.Web pour Linux** s'affiche sur une page spécifique.



Pour ouvrir la page sur laquelle vous pouvez gérer la quarantaine, cliquez sur le bouton dans le panneau de navigation.

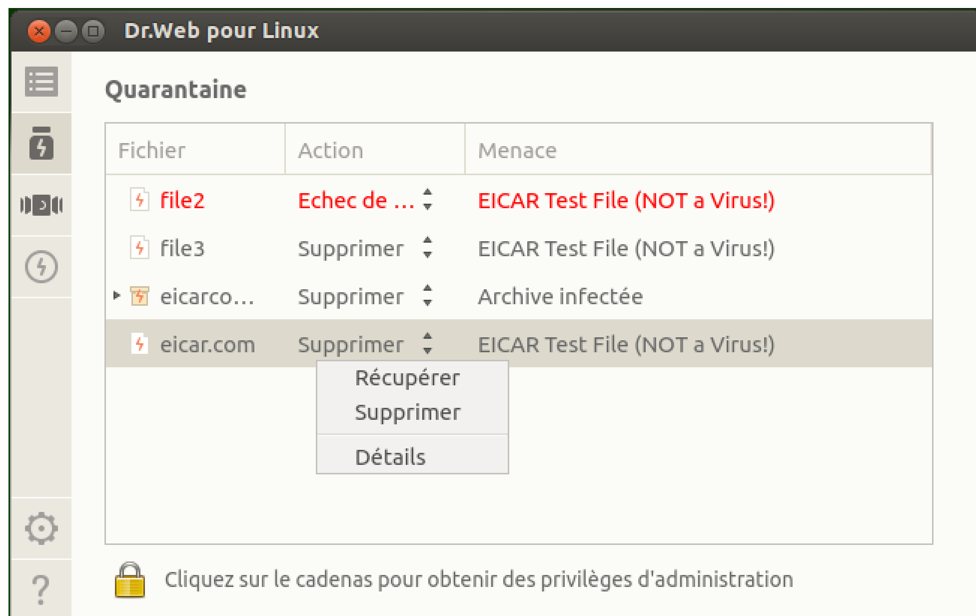


Image 35. Page de gestion de la quarantaine

Si la quarantaine n'est pas vide, les informations suivantes s'affichent pour chaque menace détectée :

- Nom de l'objet infecté
- Action à appliquer à l'objet placé en quarantaine
- Nom de la menace (d'après la classification de **Doctor Web**)

Appliquer des actions aux objets isolés

Pour appliquer une action à un objet en quarantaine, cliquez droit sur la ligne donnant l'information sur l'objet isolé et choisissez une action dans le menu qui s'est affiché. Pour appliquer une action à plusieurs objets, sélectionnez-les avec la souris en maintenant appuyées les touches CTRL ou SHIFT.

- Lorsque vous maintenez appuyée la touche CTRL, les objets isolés sont sélectionnés un par un.
- Lorsque vous maintenez appuyée la touché SHIFT, les objets isolés sont sélectionnés tous ensemble.

Les actions suivantes sont disponibles pour les objets isolés :

- **Restaurer** – restaurer l'objet isolé dans son emplacement d'origine
- **Supprimer** – supprimer définitivement l'objet

Si l'action choisie est appliquée avec succès à l'objet, il est supprimé du tableau. Si la tentative d'appliquer une action échoue, la ligne dans la liste des objets en quarantaine s'affiche en rouge et un message d'erreur apparaît dans le champ **Action**.



Si nécessaire, élevez les privilèges du logiciel pour permettre une neutralisation réussie des menaces.

Voir les données sur les objets isolés

Pour obtenir des détails sur un objet isolé, cliquez droit sur la ligne d'information sur l'objet puis cliquez sur **Détails** dans le menu qui s'est affiché. Ensuite, une fenêtre s'ouvre contenant les informations détaillées sur l'objet placé en quarantaine. Pour voir les informations sur plusieurs objets à la fois,



sélectionnez-les avec la souris tout en maintenant appuyée la touche CTRL.

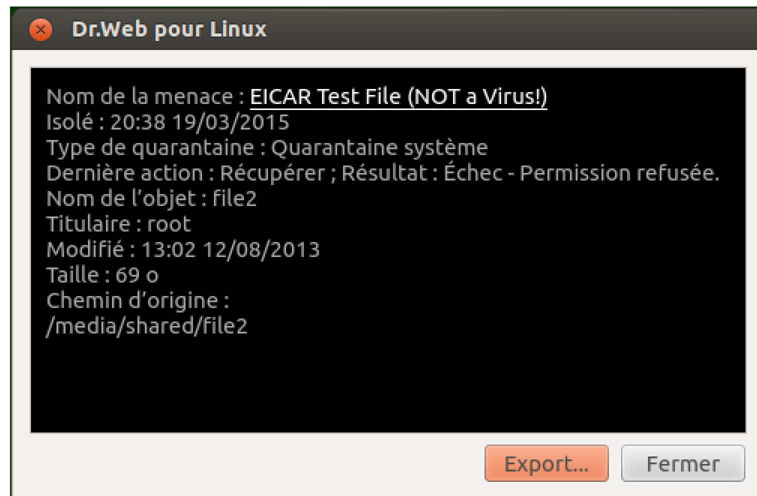


Image 36. Information sur un objet placé en quarantaine

La fenêtre affiche les informations suivantes :

- Nom de la menace (selon la classification de**Doctor Web**)
- Date et heure du déplacement de l'objet en quarantaine
- Type de dossier de quarantaine dans lequel l'objet a été déplacé
- Dernière action appliquée à l'objet et résultat de cette action
- Nom du composant **Dr.Web pour Linux** qui a détecté la menace
- Détails sur l'objet isolé : nom de l'objet, nom du propriétaire, dernière date de modification et chemin vers l'objet dans le système de fichiers

Cliquer sur le lien du nom de la menace ouvre une page web donnant des informations sur la menace dans votre navigateur (un nom de menace est un lien vers le site officiel de **Doctor Web** ; une connexion Internet valide est requise). Vous pouvez sauvegarder l'information affichée vers un fichier texte en cliquant sur le bouton **Exporter...** (une fois le bouton cliqué, un sélecteur de fichiers va s'ouvrir).

Pour fermer la fenêtre, cliquez sur **Fermer**.

Mise à jour des bases virales

Des mises à jour régulières des bases virales et du moteur **Dr.Web pour Linux** sont téléchargées et installées par **l'Updater** automatiquement Vous pouvez consulter les statistiques des bases virales et forcer leur mise à jour sur une page spéciale de la fenêtre de **Dr.Web pour Linux**. Pour ouvrir la page, cliquez sur **Dernière mise à jour** sur la page Principale.



Image 37. Page de gestion des mises à jour

La page affiche les informations suivantes :

- Statut de la base virale
- Données sur la dernière mise à jour et heure de la prochaine mise à jour planifiée

Pour forcer une mise à jour de la base, cliquez sur **Mettre à jour**. Pour fermer la page de gestion des mises à jour, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.



Si **Dr.Web pour Linux** fonctionne en mode Protection centralisée et que le serveur de protection centralisée a désactivé les mises à jour manuelles en conformité avec la politique de sécurité du réseau antivirus, la page de gestion des mises à jour peut être bloquée.

Configurer les mises à jour

Vous pouvez configurer les paramètres de mise à jour de **Dr.Web pour Linux** sur la page des paramètres à l'onglet **Principal**.

Problèmes de l'Updater

Si un échec de **l'Updater** est constaté, une alerte d'erreur s'affiche sur la page de gestion des mises à jour. Pour résoudre le problème, consultez l'Annexe D, où vous pouvez trouver une description détaillée des erreurs connues.

Gestionnaire de Licences

En mode graphique, le **Gestionnaire de Licences** permet de consulter les informations sur la version en cours de l'utilisateur de **Dr.Web pour Linux** Les données de licence sont stockées dans un fichier clé de licence qui permet le fonctionnement de **Dr.Web pour Linux** sur l'ordinateur de l'utilisateur. Si aucun fichier clé de licence ni fichier clé de démo n'est trouvé sur l'ordinateur, toutes les fonctionnalités de **Dr.Web pour Linux** (y compris la vérification des fichiers, le contrôle du système de fichiers et la mise à jour de la base virale) sont bloquées.

Gestionnaire de licences

La page du **Gestionnaire de Licences** est disponible dans l'interface graphique de **Dr.Web pour Linux** Pour ouvrir le page du Gestionnaire de licences, cliquez sur le bouton **Licence** sur la page Principale.



Si un fichier clé de démo ou de licence pour **Dr.Web pour Linux** est trouvé, la page de démarrage du **Gestionnaire de Licences** affiche les informations sur la licence, incluant le numéro de licence, le propriétaire de la licence et la durée de validité. Ces informations sont récupérées du fichier clé correspondant.

L'image ci-dessous montre l'apparence de la page du **Gestionnaire de Licences**.



Image 38. Page d'information sur la licence

Pour supprimer un fichier clé de licence, cliquez sur la croix près du numéro de licence.

Vous pouvez fermer le **Gestionnaire de Licences** à tout moment, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.

Activation de la licence

Pour activer une licence via le **Gestionnaire de Licences** et obtenir le fichier clé correspondant fournissant les fonctionnalités de **Dr.Web pour Linux** (incluant l'achat d'une nouvelle licence ou le renouvellement de la licence en cours) ou obtenir une version démo, cliquez sur **Obtenir une nouvelle licence...**. L'assistant d'enregistrement s'ouvre. Notez que l'assistant d'enregistrement s'ouvre automatiquement uniquement au premier démarrage de **Dr.Web pour Linux** après son installation.

A la première étape, choisissez le type d'activation qui peut être l'un des suivants :

1. Activation d'une licence ou d'une démo en utilisant un numéro de série
2. Obtention d'une version démo
3. Installation d'un fichier clé obtenu précédemment
4. Activation de **Dr.Web pour Linux** via le serveur de protection centralisée



Pour enregistrer un numéro de série et obtenir un fichier clé de démo, une connexion Internet valide est requise.

1) Activation d'une licence ou d'une démo en utilisant un numéro de série

Pour activer une licence ou une version démo en utilisant un numéro de série, il faut entrer les caractères du numéro de série reçu à l'achat du produit dans le champ et cliquer sur **Activer**.



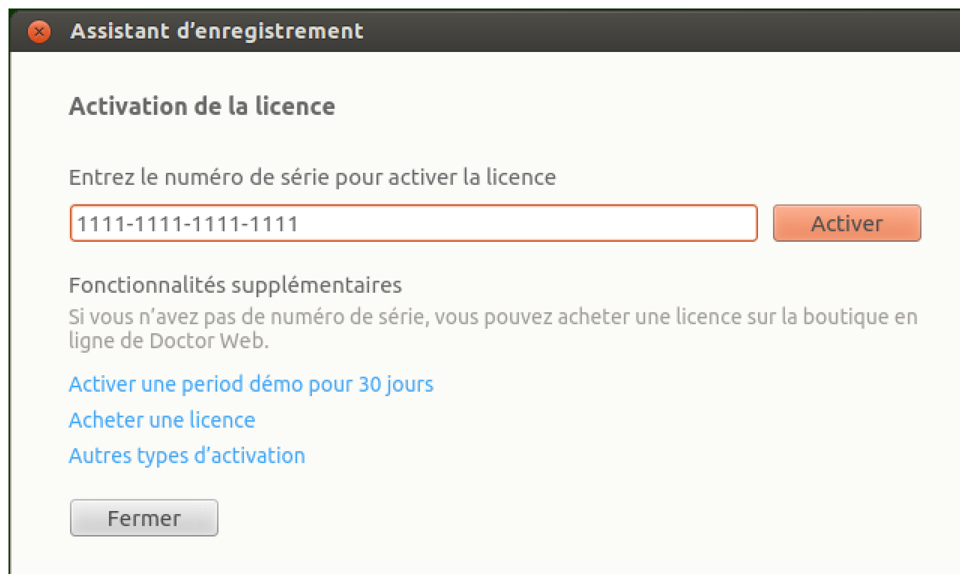


Image 39. Enregistrement en utilisant un numéro de série



Si vous ne possédez pas de numéro de série ou de fichier clé valide, vous pouvez acheter une licence sur le site officiel de **Doctor Web** Pour ouvrir la page de la boutique en ligne, cliquez sur **Acheter une licence.**

Pour en savoir plus sur les autres moyens d'acheter une licence pour les produits **Dr.Web**, consultez la section Licencing.

Après avoir cliqué sur le bouton **Activer**, la connexion avec le serveur d'enregistrement de **Doctor Web** est établie.

Si le numéro de série que vous avez indiqué à la première étape a été obtenu via le site web de **Doctor Web** et délivré pour une période de démo de trois mois, les étapes suivantes ne sont pas requises pour son activation.

Si le numéro de série indiqué correspond à une licence pour utiliser **Dr.Web pour Linux** sur deux ordinateurs, vous devez indiquer sur combien d'ordinateurs vous souhaitez utiliser le produit. Si vous choisissez **Sur deux ordinateurs,** vous pouvez activer le deuxième numéro de série de ce kit sur un autre ordinateur et obtenir le deuxième fichier clé. Dans ce cas la durée de validité des licences sur les deux ordinateurs sera la même (par exemple, un an). Si vous choisissez **Sur un ordinateur,** vous serez invité d'indiquer le deuxième numéro de série du kit. Vous ne pourrez plus utiliser ce numéro de série sur un autre ordinateur (ainsi que la copie du fichier clé de licence, reçu après l'activation de la licence unie), mais la durée de validité de licence sera doublée (par exemple, jusqu'a deux ans si votre licence est valide pour un an).



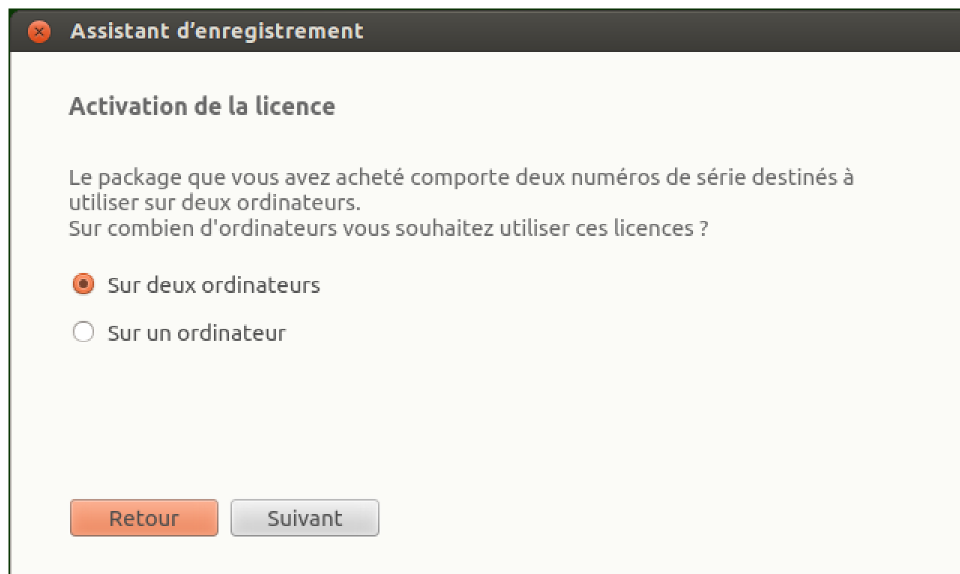


Image 40. Sélectionner le nombre d'ordinateurs

Après avoir sélectionné le nombre d'ordinateurs sur lesquels vous souhaitez activer la licence, cliquez sur **Suivant**, si vous avez choisi **Sur un ordinateur,** indiquez le deuxième numéro de licence du kit sur la page affichée de l'Assistant. Ensuite cliquez sur **Suivant.**

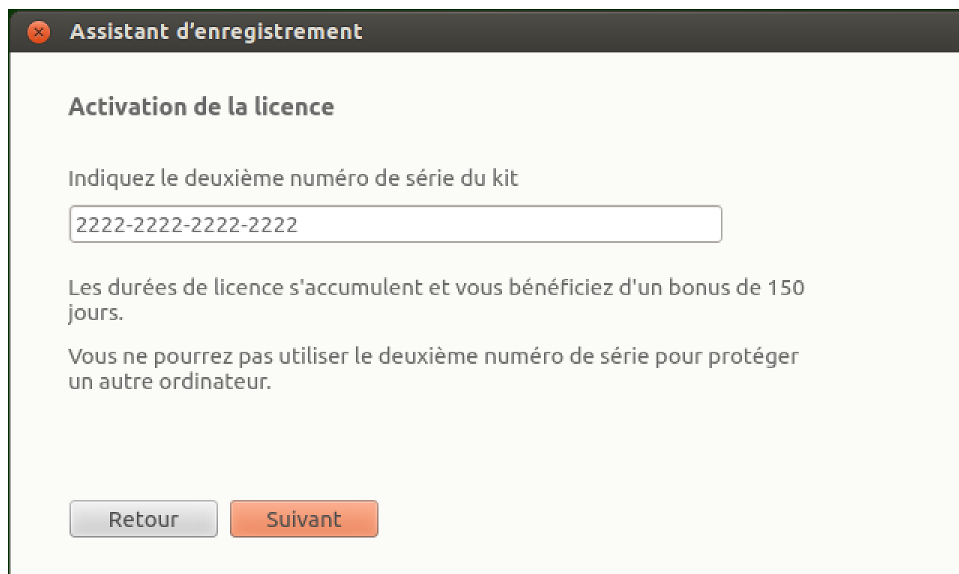


Image 41. Indication du deuxième numéro de licence

Puis vous serez invité à obtenir le bonus de 150 jours ajoutés à la durée de validité de votre nouvelle licence. Pour ce faire, veuillez indiquer des informations concernant la licence précédente si vous en possédez une. Si vous voulez obtenir le bonus, sélectionnez **Indiquez licence précédente,** si vous ne voulez pas obtenir le bonus ou vous n'avez pas de licence précédente, sélectionnez **Je n'ai pas de licence précédente** et cliquez sur **Suivant**.



Assistant d'enregistrement

+150 jours à votre licence

Si vous avez déjà utilisé une licence Dr.Web d'au moins 6 mois, vous bénéficiez d'un bonus – 150 jours ajoutés à la durée de votre nouveau fichier clé de licence.

Indiquez licence précédente

Je n'ai pas de licence précédente

Retour Suivant

Image 42. Obtenir le bonus

Si à la première étape vous avez indiqué le numéro special de renouvellement, vous serez invité d'indiquer la licence précédente pour ne pas perdre le bonus de 150 jours ajoutés à la nouvelle licence. Si dans ce cas vous sélectionnez **Je n'ai pas de licence précédente**, vous diminuez de 150 jours la durée de validité de votre nouvelle licence.

Assistant d'enregistrement

Renouvellement de la licence

Le numéro de série 1111-1111-1111-1111 est destiné au renouvellement de la licence. Cela signifie que pour continuer l'enregistrement du produit, vous devez confirmer que vous avez déjà utilisé la version sous licence du produit Dr.Web pour 6 mois minimum.

Indiquez licence précédente

Je n'ai pas de licence précédente
Je suis d'accord pour réduire ma période de licence par 150 jours.

Retour Suivant

Image 43. Renouvellement de licence

Si vous avez sélectionné **Indiquez licence précédente,** veuillez indiquer le numéro de licence précédente et le chemin vers le fichier clé dans la fenêtre affichée.

Assistant d'enregistrement

Indiquez licence précédente

Numéro de série : 3333-3333-3333-3333

La licence indiquée sur cette étape sera bloquée.
Veuillez ne pas indiquer la licence que vous prévoyez d'utiliser plus tard.

Si la durée de cette licence est de 6 mois au minimum, vous bénéficiez d'un bonus de 150 jours pour la nouvelle licence.

Retour Suivant

Image 44. Indication de licence précédente

Si vous indiquez une licence qui n'a pas expiré, la durée de la licence activée sera étendue avec la durée de validité restante de la licence précédente et le bonus de 150 jours. Si vous activez une licence avec deux numéros de série, le bonus sera appliqué en fonction de l'option que vous avez sélectionnée à l'étape précédente.

- **Sur deux ordinateurs**, et cet ordinateur est le premier. Pour activer le bonus de 150 jours pour le premier ordinateur, indiquez la licence précédente délivrée pour cet ordinateur (s'il y en a un). N'indiquez pas le second numéro de série de la licence précédente ici.
- **Sur deux ordinateurs,** et cet ordinateur est le second. Pour activer le bonus de 150 jours pour le second ordinateur, indiquez la licence précédente délivrée pour cet ordinateur (s'il y en a un). N'indiquez pas le premier numéro de série de la licence précédente ici.
- **Sur un ordinateur.** Dans ce cas, non seulement la durée de la licence achetée est doublée, mais elle est également étendue de 150 jours. De plus, si vous indiquez la licence précédente délivrée pour le second ordinateur, la durée doublée de la nouvelle licence sera étendue de 150 nouveaux jours (et de la durée de validité restante de la licence précédente).

Pour indiquer la précédente licence, vous pouvez soit entrer son numéro de série dans le champ correspondant, soit donner son fichier clé. Sélectionnez le type de l'information concernant la licence précédente dans la liste déroulante située à gauche du champ d'entrée. Pour indiquer le fichier clé, faites une des actions suivantes :

- Indiquez le chemin vers le fichier dans le champ « entrée »
- Indiquez le fichier via le sélecteur de fichiers standard en cliquant sur le bouton **Parcourir**
- Glissez/déposez le fichier depuis la fenêtre du gestionnaire de fichiers dans la fenêtre de l'Assistant d'enregistrement

Notez que vous pouvez indiquer l'archive zip contenant le fichier clé sans le décompresser.

Pour continuer l'enregistrement, cliquez sur **Suivant.**

A l'étape suivante, indiquez vos données d'enregistrement incluant :

- Nom d'enregistrement
- Votre région (pays), sélectionnée dans la liste
- Email adresse valide

Tous les champs du formulaire d'enregistrement sont obligatoires.

Assistant d'enregistrement

La dernière étape

Indiquez les données du titulaire de la licence afin d'achever l'activation.

Nom d'enregistrement — User Name

Lieu — France

Adresse email — user@usermail.dom

Retour | Terminé

Image 45. Page d'information de l'utilisateur

Après avoir rempli tous les champs correctement, cliquez sur **Terminé** pour établir une connexion serveur et obtenir un fichier clé de licence. Si nécessaire, vous pouvez utiliser le fichier clé de licence sur un autre ordinateur après l'avoir supprimé de cet ordinateur.

2) Obtenir une version démo

Si vous souhaitez activer une version démo qui fournit les fonctionnalités complètes des composants **Dr.Web pour Linux** pour une période de 30 jours, cliquez sur **Activer une periode démo pour 30 jours** à la première étape.



Lors de l'activation de la version démo pour un mois, vous n'avez pas besoin de fournir des données personnelles. Cependant, vous pouvez vous enregistrer sur le site officiel de **Doctor Web** et obtenir un numéro dé série pour une version démo de trois mois. Il est possible d'obtenir une autre version démo pour le même ordinateur après un certain délai.

Pour en savoir plus, consultez la section Licencing.

3) Installation d'un fichier clé obtenu antérieurement

Si vous possédez déjà une licence valide et le fichier clé qui lui est lié (par exemple, obtenu auprès de **Doctor Web** ou des partenaires de **Doctor Web** via email), vous pouvez activer **Dr.Web pour Linux** en installant ce fichier clé. Pour cela, cliquez sur **Autres types d'activation** à la première étape et indiquez le chemin vers le fichier clé dans la case qui s'affiche.





Image 46. Activation en utilisant le fichier clé

Pour indiquer le fichier clé, faites une des actions suivantes :

- Indiquez le chemin vers le fichier dans le champ « entrée »
- Indiquez le fichier via le sélecteur de fichiers standard en cliquant sur le bouton **Parcourir**
- Glissez/déposez le fichier depuis la fenêtre du gestionnaire de fichiers dans la fenêtre de l'Assistant d'enregistrement

Notez que vous pouvez indiquer l'archive zip contenant le fichier clé sans le décompresser.

Après avoir indiqué le chemin vers le fichier clé (ou le chemin vers l'archive contenant le fichier clé), cliquez sur **Terminé** pour installer le fichier clé automatiquement Si nécessaire, le fichier clé est automatiquement décompressé et copié dans le répertoire des fichiers de **Dr.Web pour Linux**. Une connexion Internet n'est pas requise.

4) Activation de l'antivirus via le serveur de protection centralisée

Vous pouvez activer votre **Dr.Web pour Linux** en le connectant au serveur de protection centralisée qui permet l'administration centralisée du réseau antivirus. Dans ce cas, le serveur génère un fichier clé requis pour le fonctionnement de **Dr.Web pour Linux**. Choisissez ce type d'activation uniquement si le fournisseur ou l'administrateur du réseau de l'entreprise ont délivré un fichier spécial contenant les paramètres de connexion de votre **Dr.Web pour Linux** au serveur de protection centralisée.

Pour connecter **Dr.Web pour Linux** au serveur de protection centralisée, cliquez sur **Autres types d'activation** à la première étape, indiquez le chemin vers le fichiers contenant les paramètres de connexion (pareil à l'activation avec l'utilisation du fichier clé, décrite dans l'acticle précédent).

Pour indiquer le fichier contenant les paramètres de connexion, faites une des actions suivantes :

- Indiquez le chemin vers le fichier dans le champ « entrée »
- Indiquez le fichier via le sélecteur de fichiers standard en cliquant sur le bouton **Parcourir**
- Glissez/déposez le fichier depuis la fenêtre du gestionnaire de fichiers dans la fenêtre de l'Assistant d'enregistrement

Notez que vous pouvez indiquer l'archive zip contenant le fichier contenant les paramètres de connexion sans le décompresser.

Après avoir indiqué le chemin vers le fichier contenant les paramètres (ou l'archive contenant ce fichier), cliquez sur **Terminé** pour établir la connexion au serveur de protection centralisée (une



connexion réseau est requise).

Après la fin de la procédure de l'activation (quel que soit le type d'activation choisi), la dernière page de l'Assistant avec les notifications correspondantes s'affiche. Cliquez sur **OK** pour quitter l'Assistant et ouvrez la page Principale de **Dr.Web pour Linux**.



Image 47. Notification de succès de l'activation

Si une erreur est survenue à n'importe quelle étape de la procédure, une page avec une notification décrivant rapidement l'erreur s'affiche. L'image ci-dessous en montre un exemple.



Image 48. Message d'erreur

Si une erreur survient, vous pouvez retourner à l'étape précédente et faire des corrections (par exemple, corriger le numéro de série ou indiquer un chemin correct). Pour retourner à l'étape précédente, cliquer sur **Retour**.

Si l'erreur est due à un problème temporaire (par exemple, un échec réseau temporaire), vous pouvez tenter de recommencer l'opération en cliquant sur **Réessayer**. Si nécessaire, vous pouvez cliquer sur **Fermer** pour annuler l'enregistrement et quitter l'Assistant. Dans ce cas, vous devez recommencer l'enregistrement ultérieurement. Si l'Assistant d'enregistrement ne pourra pas se connecter au serveur

d'enregistrement de **Doctor Web** pour vérifier le numéro de série, un message d'erreur sera affiché.



Image 49. Erreur de connexion au serveur d'enregistrement

Si l'erreur est liée à l'impossibilté de vous connecter via Internet, mais vous pouvez vous connecter via le serveur proxy, le passage par le lien **Paramètres du serveur proxy** affiche la fenêtre de paramètres du serveur-proxy:

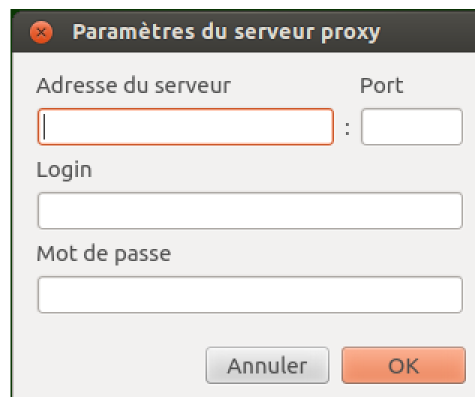


Image 50. Paramètres du serveur proxy

Dans cette fenêtre il est nécessaire de spécifier les paramètres d'accès au serveur proxy et cliquer sur **OK** Puis il faut réessayer de se connecter au serveur d'enregistrement de **Doctor Web**, en cliquant sur **Réessayer**.



Notez que lors de l'activation d'une nouvelle licence et la génération d'un nouveau fichier clé, le fichier clé précédent utilisé par **Dr.Web pour Linux**, est automatiquement stocké comme copie de sauvegarde dans le répertoire `/etc/opt/drweb.com`.

Si nécessaire, vous pouvez réutiliser ce fichier clé en l'installant.

Supprimer un fichier clé de licence

Si nécessaire (par exemple si vous décidez d'utiliser **Dr.Web pour Linux** sur un autre ordinateur), vous pouvez supprimer un fichier clé de licence installé gérant le fonctionnement de **Dr.Web pour Linux**. Pour cela, ouvrez la page d' information sur la licence (la page de démarrage du **Gestionnaire de Licences**) et cliquez sur l'icône de la croix près du numéro de la licence en cours.

Ensuite, confirmez la suppression du fichier clé de licence dans la fenêtre qui s'ouvre en cliquant sur **Oui**. Si vous souhaitez annuler la suppression, cliquez sur **Non**.

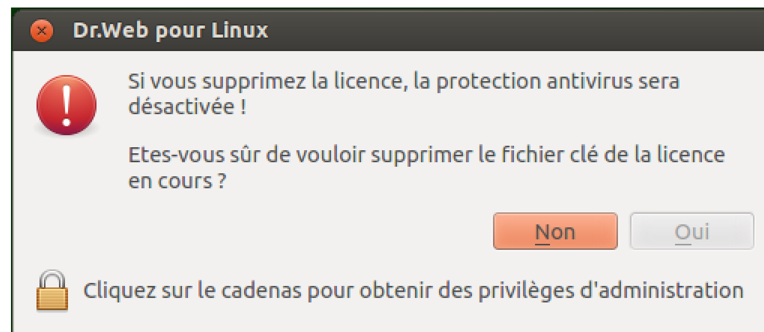


Image 51. Fenêtre de confirmation avant de supprimer un fichier clé de licence



Pour supprimer un fichier clé de licence, le logiciel doit être démarré avec les privilèges de superuser. Si le logiciel ne possède pas de permissions élevées, le bouton **Oui** n'est pas disponible lors de la tentative de suppression du fichier clé. Si nécessaire, vous pouvez élever les privilèges et, si cela fonctionne, le bouton **Oui** devient accessible.

La suppression d'un ficher clé de licence n'affecte pas la durée de validité de la licence. Si la licence n'a pas expiré, vous pouvez obtenir un nouveau fichier clé pour cette licence pour la durée de validité restante.

Après la suppression d'un fichier clé, toutes les fonctionnalités antivirus de **Dr.Web pour Linux** (scan de fichiers, mise à jour de la base virale, surveillance du système de fichiers) sont bloquées jusqu'à ce qu'une nouvelle licence ou version démo soit activée.

Privilèges de Gestion du Logiciel

Certaines actions avec **Dr.Web pour Linux** peuvent être effectuées en mode graphique uniquement si l'application possède des privilèges élevés *des privilèges d'administration*) qui correspondent aux droits du superuser. Ces actions sont les suivantes :

1. Gestion d'objets déplacés en *quarantaine* (c'est-à-dire dans le dossier de quarantaine qui n'est pas celui de l'utilisateur)
2. Vérification de fichiers et dossiers d'autres utilisateurs (notamment du superuser)
3. Désactiver **SpIDer Guard**
4. Désactiver **SpIDer Gate**
5. Suppression d'un fichier clé de licence, connexion et déconnexion du serveur de protection centralisée



Même si le logiciel est lancé par le superuser (par exemple, en utilisant les commandes `su` ou `sudo`), il **ne** reçoit pas de privilèges élevés par défaut.

Toutes les pages qui permettent des actions requérant des privilèges élevés présentent un bouton spécifique avec l'icône d'un cadenas. L'icône indique si le logiciel possède ou pas des privilèges de superuser :

 – Le logiciel ne possède pas de privilèges élevés.
Cliquez sur l'icône pour élever les privilèges.

 – Le logiciel possède des privilèges élevés.
Cliquez sur l'icône pour baisser les privilèges ; c'est-à-dire pour passer des privilèges



administrateur aux droits utilisateur.

Lorsque vous cliquez sur l'icône pour élever les privilèges, la fenêtre d'authentification de l'utilisateur s'ouvre.

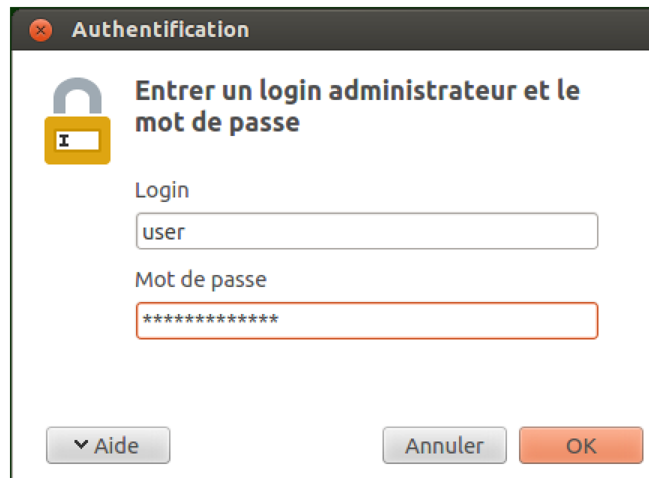


Image 52. Fenêtre d'authentification

Pour donner au logiciel des privilèges administrateur, vous devez vous authentifier en tant qu'utilisateur dont le compte est inclus au groupe administrateur de **Dr.Web pour Linux**, ou comme superutilisateur (compte système `root`) et cliquer sur **OK.** Pour annuler l'élévation de privilèges, cliquez sur **Annuler.**En cliquant sur le bouton **Aide**, un court texte décrivant comment s'authentifier s'affiche. Pour masquer le texte, cliquez de nouveau sur le bouton **Aide**.



Durant l'installation de **Dr.Web pour Linux**, un groupe d'utilisateurs qui peut élever ses droits jusqu'aux privilèges de superutilisateur (par exemple, le groupe `sudo`) est choisi comme groupe d'administrateurs. Si la tentative de recherche de ce groupe échoue, vous pouvez entrer les login et mot de passe de superutilisateur dans la fenêtre d'authentification pour élever les droits du logiciel.

Le passage des privilèges administrateur aux droits utilisateur ne requiert pas d'authentification.

Aide et références

Pour accéder au fichier Aide, cliquez  sur le panneau de navigation.

Après avoir cliqué sur le bouton, un menu pop-up avec les sujets suivants va s'ouvrir :

- **Aide** – ouvre le Manuel utilisateur de **Dr.Web pour Linux**
- **Forum** – ouvre la page web du forum officiel (une connexion Internet est requise) de**Doctor Web**
- **Support technique** – ouvre la page web (une connexion Internet est requise) du support technique de **Doctor Web**
- **Mon Dr.Web** – ouvre votre page web personnel sur le site officiel de **Doctor Web** une connexion Internet est requise)
- **A propos de** – ouvre une fenêtre avec des informations sur votre version de **Dr.Web pour Linux**

De plus, lorsqu'une des pages de la fenêtre principale de **Dr.Web pour Linux** affiche un message d'erreur, vous pouvez suivre le lien **Détails** pour obtenir des informations sur l'erreur et les conseils pour résoudre le problème.



Configurer les paramètres de fonctionnement

Dans la fenêtre des paramètres, vous pouvez configurer les paramètres du logiciel suivants :

- Périodicité des mises à jour
- Actions appliquées aux menaces détectées (à la fois par le **Scanner** lors d'un scan à la demande et par **SpIDer Guard**)
- Liste des objets à exclure des contrôles du **Scanner** et de **SpIDer Guard**
- Paramètres de contrôle de l'accès Internet
- Planification pour lancer des contrôles réguliers effectués par le **Scanner**
- Mode de protection (*Standalone*, *Protection centralisée*)
- Utilisation du service **Dr.Web Cloud**

Pour ouvrir la la fenêtre des paramètres, cliquez  sur le panneau de navigation.

Dans la la fenêtre des paramètres, les onglets suivants sont disponibles :

- Principal – ici, vous pouvez configurer les paramètres de notifications et la fréquence des mises à jour automatiques.
- Scanner – à cet onglet, vous pouvez configurer les réactions de **Dr.Web pour Linux** face aux menaces détectées durant le scan à la demande ou planifié.
- SpIDer Guard – ici, vous pouvez configurer les réactions de **Dr.Web pour Linux** aux menaces détectées par **SpIDer Guard.**
- SpIDer Gate – ici, vous pouvez configurer les paramètres du contrôle d'accès à Internet effectué par **SpIDer Gate**.
- Exclusions – ici, vous pouvez définir la liste des objets à exclure du scan à la demande, du scan d'après la planification, ou des contrôles de **SpIDer Guard**.
- Planificateur – ici, vous pouvez configurer la planification pour lancer les scans.
- Mode – ici, vous pouvez sélectionner le mode opératoire de **Dr.Web pour Linux** (Standalone, protection centralisée).
- Dr.Web Cloud – ici, vous pouvez interdire ou autoriser à **Dr.Web pour Linux** l'utilisation du service **Dr.Web Cloud.**

Pour accéder au fichier Aide, cliquez .



Toutes les modifications apportées dans ces onglets sont appliquées immédiatement.

Notez que lorsque **Dr.Web pour Linux** opère en mode Protection centralisée, certains paramètres peuvent ne pas être disponibles.

Paramètres Principaux

À l'onglet **Général**, vous pouvez configurer les paramètres principaux du logiciel.

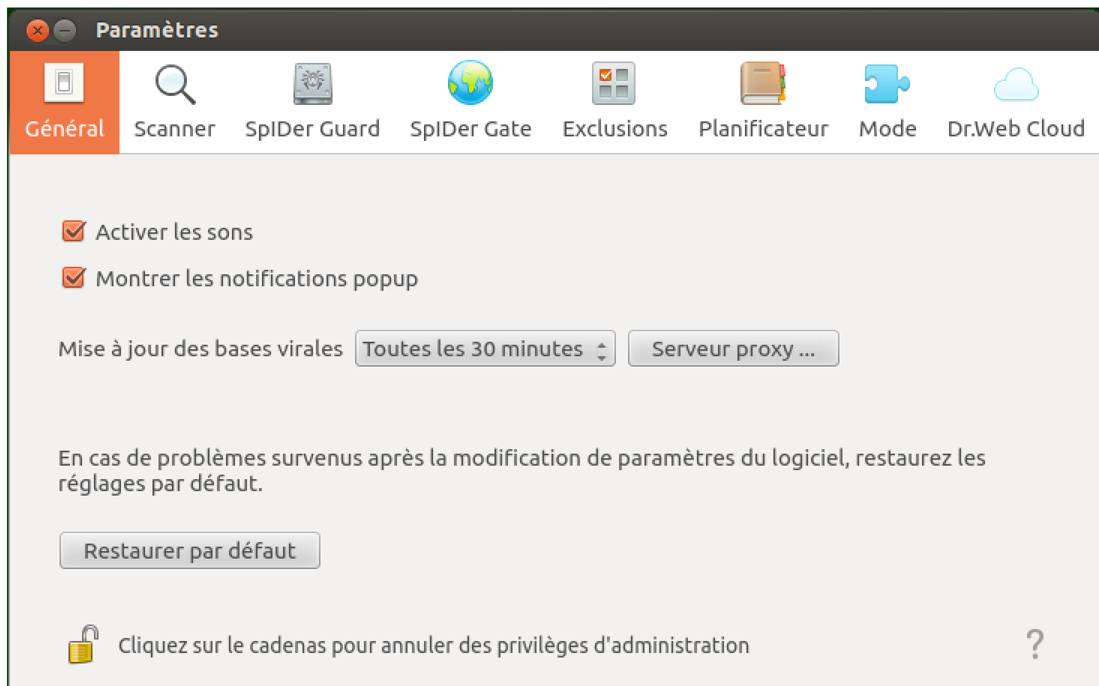


Image 53. Onglet Général

Option	Description
Activer les sons	Cochez cette case si vous souhaitez que **Dr.Web pour Linux** utilise les notifications sonores pour des événements particuliers comme • Détection d'une menace (par le **Scanner** et par **SpIDer Guard**) • Erreur de scan • Autres
Montrer les notifications pop-up	Cochez cette case si vous souhaitez que **Dr.Web pour Linux** affiche des notifications pop-up pour des événements particuliers comme • Détection de menaces • Erreur de scan • Autres
Mise à jour des bases virales	Choisissez la fréquence à laquelle **l'Updater** vérifiera la disponibilité de mises à jour pour les bases virales et le moteur de **Dr.Web pour Linux**.
Serveur proxy ...	Cliquez pour configurer les paramètres du serveur proxy pour la réception des mises à jour (**l'Updater** utilise un serveur proxy si le contact avec des serveurs externes est interdit par la politique de sécurité réseau).
Restaurer par défaut	Cliquez pour restaurer les paramètres par défaut.



Pour gérer les paramètres de mise à jour et les restaurer par défaut, le logiciel doit posséder des privilèges de superuser. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.



Configurer le Serveur Proxy pour les Mises à jour

Dans la fenêtre des paramètres permettant de configurer l'utilisation d'un serveur proxy par **l'Updater**, vous pouvez

- Activer ou désactiver l'utilisation du serveur proxy pour recevoir les mises à jour.
- Indiquer l'adresse du serveur proxy utilisée pour recevoir les mises à jour.
- Indiquer le port utilisé pour se connecter au serveur proxy.
- Indiquer le nom et mot de passe de l'utilisateur utilisé pour l'authentification sur le serveur proxy.



Image 54. Paramètres du serveur proxy

Cliquez sur **OK** pour conserver les modifications et fermer la page ou sur **Annuler** pour les refuser.

Paramètres du Scanner

À l'onglet **Scanner**, vous pouvez définir les actions que **Dr.Web pour Linux** applique aux menaces détectées lors du scan de fichiers à la demande de l'utilisateur ou programmé.



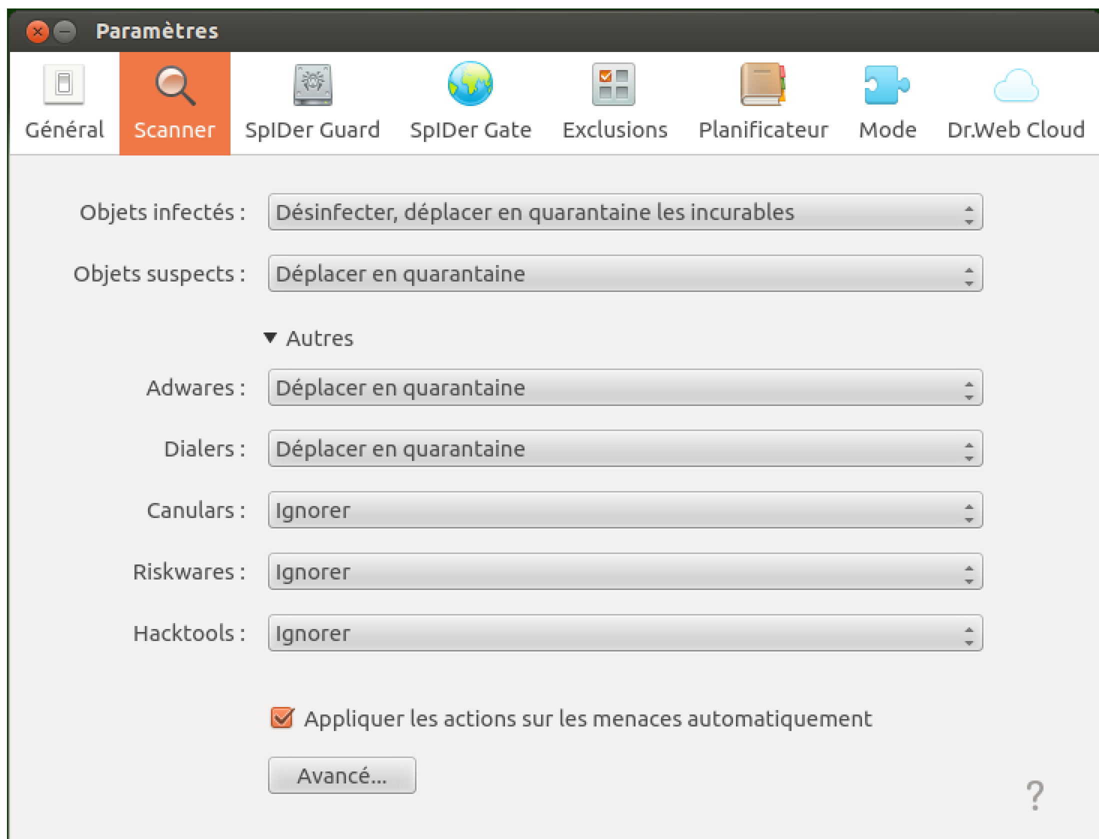


Image 55. Onglet paramètres du Scanner

Dans la liste déroulante, choisissez une action que va appliquer **Dr.Web pour Linux** à une menace d'un certain type.

Si vous souhaitez que **Dr.Web pour Linux** applique des actions spécifiques aux objets malveillants immédiatement après la détection d'une menace, cochez la case **Appliquer les actions sur les menaces automatiquement**. Dans ce cas, l'utilisateur est notifié sur la neutralisation et des informations sur la menace neutralisée sont ajoutées à liste des menaces). Si la case n'est pas cochée, le **Scanner** ajoute une menace détectée à la liste et l'utilisateur sélectionne manuellement l'action qui doit être appliquée.

Pour ouvrir la fenêtre des paramètres de scan avancés, cliquez sur le bouton **Avancé**.

Paramètres de scan avancés

Dans la fenêtre des paramètres avancés, vous pouvez configurer les paramètres du **Scanner** comme :

- Activer ou désactiver le scan du contenu des conteneurs
  - Archives
  - Fichiers email
- Définir la durée maximum de scan d'un fichier.

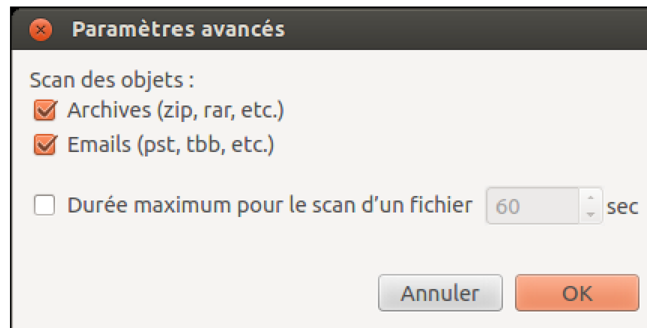


Image 56. Paramètres de scan avancés



Si les cases ne sont pas cochées, les conteneurs seront également scannés, mais uniquement comme des objets globaux, sans analyse de leur structure interne.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre ou sur **Annuler** pour les refuser.

Paramètres de SpIDer Guard

À l'onglet **SpIDer Guard**, vous pouvez définir des actions à appliquer aux menaces par le moniteur **SpIDer Guard**.

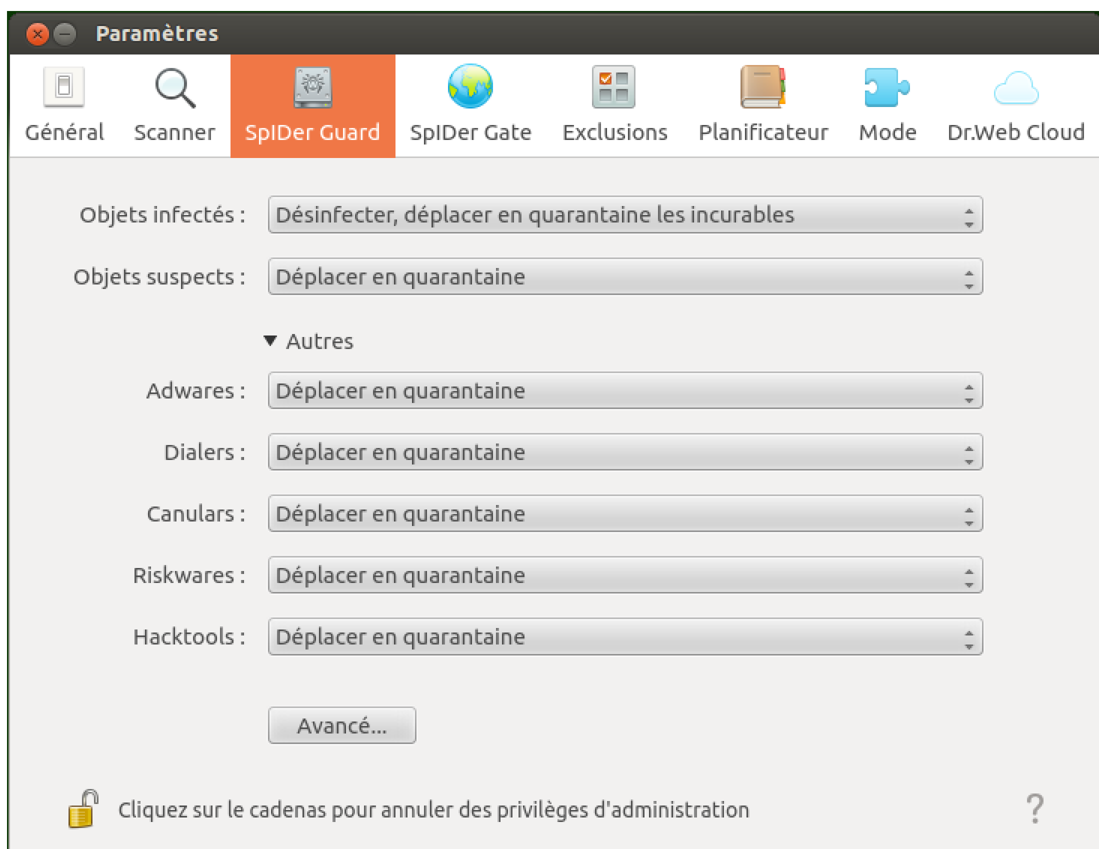


Image 57. Onglet paramètres de SpIDer Guard

Les options disponibles à l'onglet sont identiques à celles de l'onglet Scanner tab.





Le réglage des paramètres de **SpIDer Guard** demande que le logiciel possède des privilèges élevés. Pour en savoir plus, consultez la section Gestion des Droits du Logiciel.

Si **Dr.Web pour Linux** opère en mode Protection centralisée, ces paramètres sont activés en fonction des permissions indiquées sur le serveur.

Paramètres de SpIDer Gate

À l'onglet **SpIDer Gate**, vous pouvez configurer les politiques de sécurité que doit utiliser **SpIDer Gate** lors du contrôle de l'accès Internet.



Image 58. Onglet paramètres de SpIDer Gate

En cochant ou décochant les options, vous pouvez activer ou désactiver l'accès aux sites web des catégories suivantes :

Catégorie	Description
URL listées suite à une requête d'un propriétaire de copyright	Les sites web dont le contenu viole le copyright (d'après son propriétaire), par exemple, les répertoires de fichiers de référence, les services d'hébergement de fichiers.
Sites non recommandés	Les sites web au contenu douteux (suspecté de phishing ou de vol de mot de passé, etc.).
Sites pour adultes	Sites web avec du contenu pour adultes
Sites consacrés à la violence	Sites web dont le contenu traite d'actes violents (par exemple actes de terrorisme, images de scènes de guerre etc.).
Sites consacrés aux armes	Sites dont le contenu donne des informations sur les armes et les explosifs.
Sites consacrés aux jeux d'argent	Sites web de casinos Internet, jeux d'argent et paris.
Sites consacrés aux drogues	Sites web dont le contenu traite de production, distribution et consommation de drogues.
Langage obscène	Sites web dont le contenu emploie un langage obscène.



Catégorie	Description
Chats	Sites web de chat.
Sites consacrés au terrorisme	Sites web dont le contenu décrit en détail des actes terroristes, la fabrication d'explosifs ou des contenus visant à promouvoir une propagande terroriste.
Email	Sites web proposant la création d'email gratuit.
Réseaux sociaux	Sites web de réseaux sociaux.



Les URLs qui tombent dans ces catégories sont fournies avec **Dr.Web pour Linux** et sont mises à jour automatiquement lors des mises à jour des bases virales. Les utilisateurs ne peuvent pas modifier ces listes d'URLs.

Le même site web peut appartenir à plusieurs catégories. Si c'est le cas, **SpIDer Gate** bloque son accès si l'URL est incluse à au moins une des listes.

Si vous souhaitez bloquer l'accès à un site web qui n'appartient pas à ces catégories, ajoutez-le à la liste noire utilisateur. Si, en revanche, vous souhaitez permettre l'accès à un site web bloqué inclus à une des listes noires susmentionnées, ajoutez-le à la liste blanche utilisateur.



Il existe également une autre catégorie de sites web : les sites web au contenu douteux. L'accès à ces sites est toujours bloqué, même s'ils sont ajoutés à la liste blanche de l'utilisateur.

Gérer les listes noire et blanche de sites web

Pour configurer les listes noire et blanche de l'utilisateur, cliquez sur le bouton **Listes noire et blanche**.

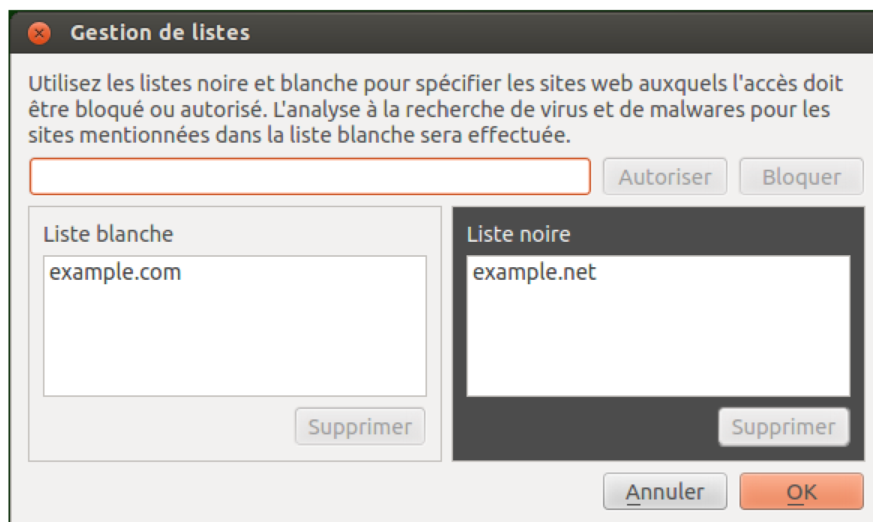


Image 59. Gestion des listes noire et blanche

Pour ajouter un site à une liste noire ou blanche, entrez l'adresse du domaine dans le champ texte et cliquez sur le bouton approprié.

- Cliquez sur **Autoriser** pour ajouter l'adresse indiquée à la liste blanche.
- Cliquez sur **Bloquer** pour ajouter l'adresse indiquée à la liste noire.

Ajouter une adresse de domaine aux listes noire ou blanche bloque ou autorise toutes les ressources de ce domaine.

Pour supprimer un élément d'une des listes, sélectionnez-le et cliquez sur **Supprimer**.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK.** Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

Configurer les paramètres de scan de fichiers

Pour configurer les paramètres de **SpIDer Gate** pour la vérification de fichiers téléchargés, cliquez sur **Avancé**

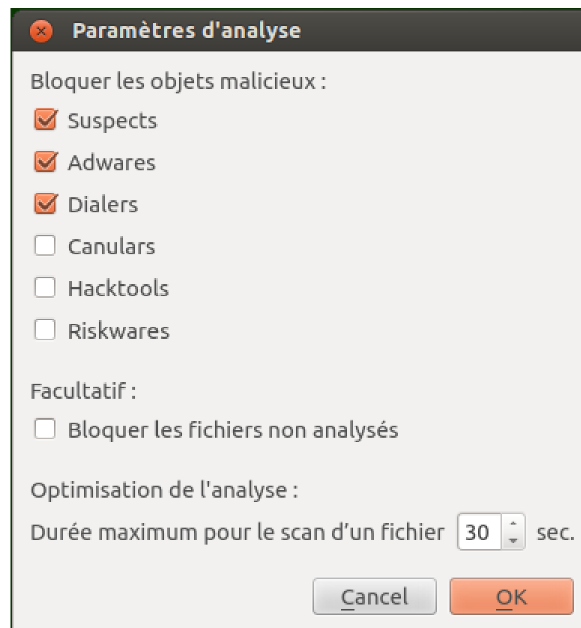


Image 60. Configurer les paramètres de vérification de fichiers

Dans la fenêtre qui s'ouvre, vous pouvez choisir les catégories d'objets malveillants à bloquer lorsqu'il y a un risque qu'ils soient téléchargés sur Internet. Si une case est cochée, les fichiers tombant dans cette catégorie seront rejetés. Si une case n'est pas cochée, les fichiers qui tombent dans cette catégorie peuvent être téléchargés. Vous pouvez également indiquer la durée maximum de scan d'un fichier téléchargé. Si l'option **Bloquer les fichiers non vérifiés** est sélectionnée, les fichiers qui ne sont pas vérifiés à cause d'une erreur sont bloqués et ne peuvent pas être téléchargés. Pour autoriser le téléchargement de tels fichiers, décochez la case (non recommandé).



Si le scan d'un fichier téléchargé a échoué parce que le délai d'analyse a expiré, ce fichier ne sera pas traité comme non vérifié et ne sera pas bloqué même si la case **Bloquer les fichiers non vérifiés** est cochée.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK.** Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.



Pour configurer les paramètres de contrôle de l'accès Internet, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.

Exclusions

À l'onglet **Exclusions** , vous pouvez indiquer les chemins vers les objets que vous souhaitez exclure du scan à la demande de l'utilisateur et/ou programmé, ainsi qu'établir une liste d'exclusions des contrôles de **SpIDer Guard**.

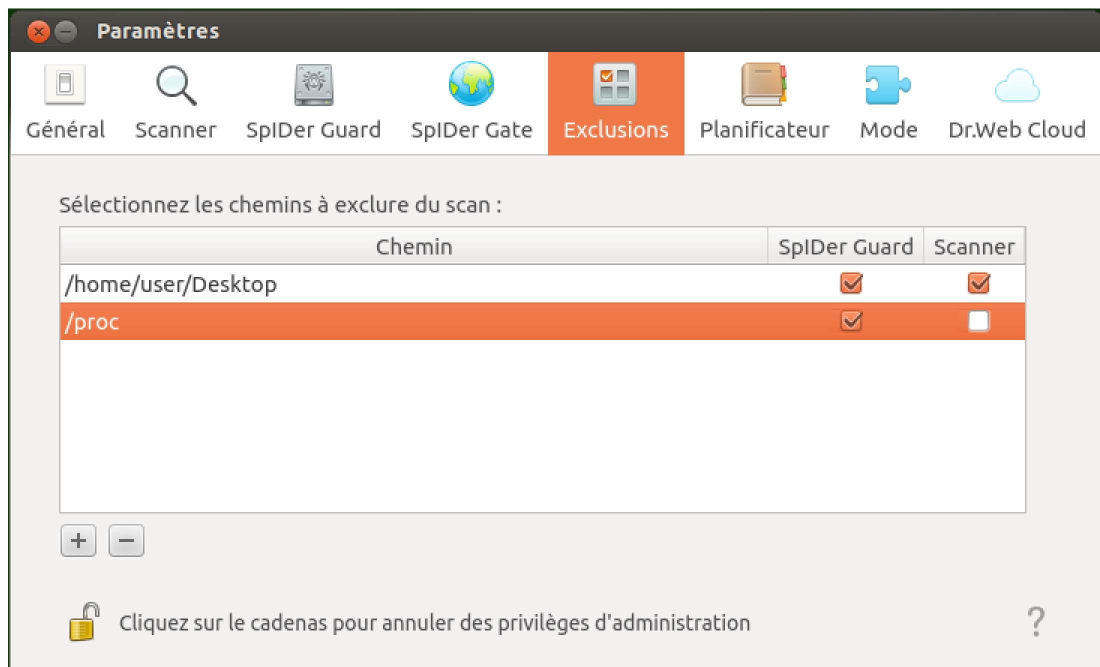


Image 61. Onglet Exclusions

Vous pouvez ajouter le même objet aux deux listes d'exclusions et désactiver son contrôle par le **Scanner** (à la demande et selon une planification) et par **SpIDer Guard**. Si un objet est ajouté à une liste d'exclusions, il est marqué d'une case dans la colonne correspondante.

Ajouter et supprimer des objets aux listes d'exclusions

Pour exclure un objet listé de l'analyse par le **Scanner** ou **SpIDer Guard**, cochez la case correspondante dans la ligne de l'objet. Pour supprimer un objet de la liste d'exclusions et permettre sa vérification, décochez la case dans la ligne de l'objet.

Pour ajouter un nouveau chemin vers un objet à la liste présentée dans cette fenêtre, cliquez sur le bouton « + » sous les chemins listés et sélectionnez le nouvel objet dans la fenêtre qui apparaît. Vous pouvez également ajouter des chemins en glissant/déposant des objets depuis la fenêtre du Gestionnaire de Fichiers.

Pour supprimer un chemin vers un objet de la liste, sélectionnez la ligne de l'objet et cliquez sur le bouton « – » sous les chemins listés.



Ajouter ou supprimer un objet de la liste d'exclusions de **SpIDer Guard** demande que le logiciel possède des privilèges élevés. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.

Notez que le chemin d'un objet ne peut pas être supprimé si l'objet est ajouté à la liste d'exclusions de **SpIDer Guard** et que le logiciel ne possède pas les permissions requises.

Paramètres du Planificateur

À l'onglet **Planificateur**, vous pouvez activer une option pour scanner les objets automatiquement d'après la planification ainsi que paramétrer cette planification et choisir le type de scan.



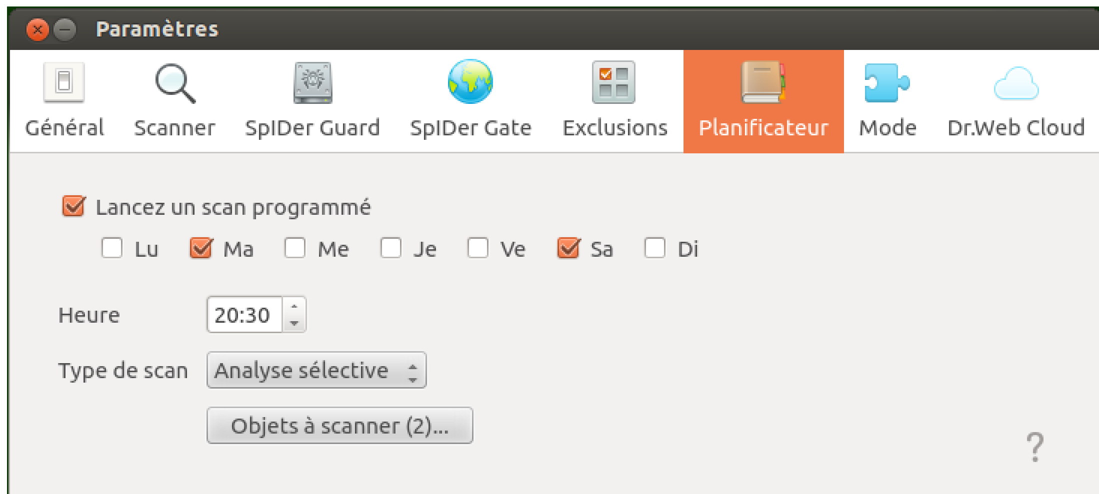


Image 62. Onglet planificateur

Pour activer des scans automatiques programmés, cochez la case **Lancer un scan programmé** Dans ce cas, **Dr.Web pour Linux** crée une tâche pour le programme **cron** pour lancer des scans périodiques.



Le programme **cron** démarre les scans aux intervalles indiqués que **Dr.Web pour Linux** soit lancé ou pas.

Si **Dr.Web pour Linux** opère en mode Protection centralisée et que le lancement des scans à la demande de l'utilisateur est interdit sur le serveur de protection centralisée, le **Scanner** ne lancera pas des scans planifiés.

Les scans lancés selon la planification ainsi que les scans à la demande sont configurés via les paramètres définis à l'onglet **Scanner**.

Configurer le scan programmé

Si le scan programmé est activé, vous pouvez configurer les paramètres suivants :

- Jours de la semaine auxquels lancer le scan (en cochant les cases correspondantes)
- Heure (heures et minutes) de démarrage du scan
- Type de scan (*Rapide*, *Complet*, ou *Personnalisé*)
- Si vous choisissez le *Scan personnalisé* , vous pouvez indiquer la liste des objets à scanner. Pour cela, cliquez sur le bouton **Objets à scanner…** (le nombre d'objets sélectionnés est indiqué entre crochets).

  Ensuite, choisissez un objet dans la fenêtre qui s'est ouverte et qui est similaire au sélecteur de fichiers pour le scan personnalisé à la demande. Vous pouvez ajouter des objets à la liste soit en cliquant sur le bouton "+", soit en les glissant/déposant depuis la fenêtre du gestionnaire de fichiers.

Pour désactiver le scan programmé, décochez la case **Lancer un scan programmé** La tâche correspondante est automatiquement supprimée de la liste de tâches du programme **cron**.

Paramètres du mode

À l'onglet **Mode**, vous pouvez connecter **Dr.Web pour Linux** au serveur de protection centralisée (en activant les modes Protection centralisée) ainsi que le déconnecter du serveur de protection centralisée (si c'est le cas, **Dr.Web pour Linux** opère en mode Standalone).



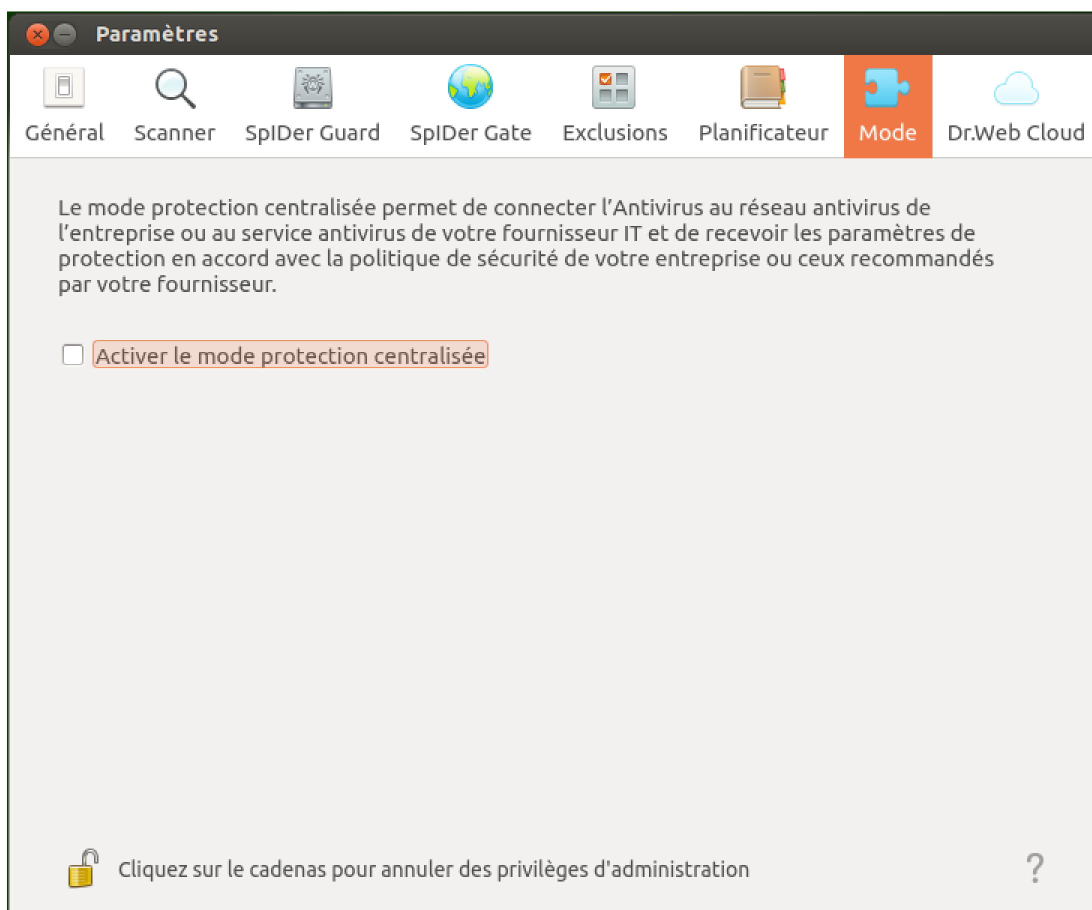


Image 63. Onglet Mode

Pour connecter **Dr.Web pour Linux** au serveur de protection centralisée depuis cet onglet, cochez la case correspondante.



Pour connecter **Dr.Web pour Linux** au serveur de protection centralisée ou l'en déconnecter, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.

Connecter au serveur de protection centralisée

Lors d'une tentative de connexion au serveur de protection centralisée, une fenêtre donnant les paramètres de connexion apparaît.

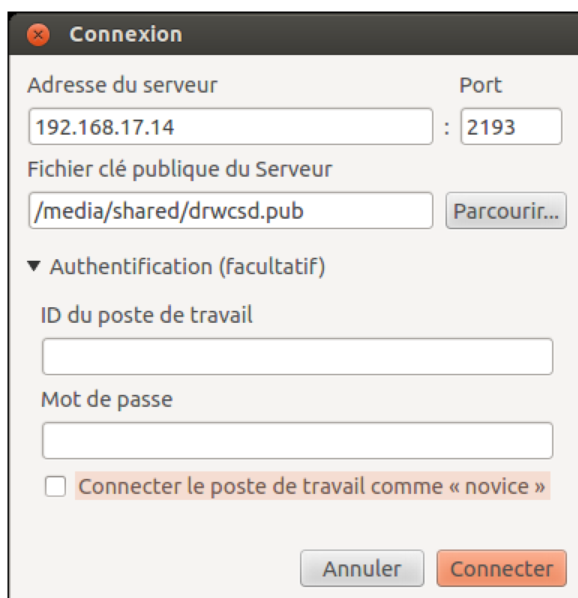


Image 64. Boîte de dialogue de connexion au serveur

Pour établir une connexion avec le serveur de protection centralisée, renseignez les paramètres suivants (fournis par l'administrateur réseau ou votre fournisseur de service Internet)

- Adresse du serveur de protection centralisée
- Port utilisé pour la connexion au serveur de protection centralisée
- Chemin vers le fichier contenant la clé publique du serveur

De plus, vous pouvez entrer l'identifiant et le mot de passe du poste de travail pour son authentification sur le serveur (s'il est connu). L'authentification sera réussie uniquement si les valeurs de la paire identifiant/mot de passe sont spécifiées. Si les champs sont vides, la connexion sera établie uniquement lorsqu'elle sera approuvée sur le serveur (automatiquement ou par l'administrateur du réseau antivirus, en fonction des paramètres du serveur).

Vous pouvez également cocher la case **Connecter un poste de travail comme « novice »**. Si c'est autorisé sur le serveur, une paire login/mot de passe unique sera automatiquement générée après l'approbation de la connexion. Notez que si cette case n'est pas cochée, une nouvelle paire de valeurs est générée même si le poste de travail possède déjà un compte sur le serveur.



Les paramètres de connexion doivent être spécifiés conformément aux instructions fournies par l'administrateur réseau ou votre fournisseur de service Internet.

Pour vous connecter au serveur, configurez tous les paramètres, cliquez sur **Connecter** et attendez que la connexion s'établisse. Pour fermer la fenêtre sans établir une connexion avec le serveur, cliquez sur **Annuler**.



Après avoir connecté **Dr.Web pour Linux** au serveur de protection centralisée, **Dr.Web pour Linux** est administré par le serveur jusqu'au passage en mode Standalone. Une connexion serveur est automatiquement établie à chaque démarrage du système d'exploitation. Pour en savoir plus, consultez la section Modes opératoires.

Veuillez noter que si le lancement du scan à la demande de l'utilisateur est interdit sur le serveur de protection centralisée, la page de lancement du scan et bouton **Scanner** de la fenêtre de **Dr.Web pour Linux** sera désactivée. De plus, dans ce cas, le **Scanner** ne lancera pas des scans planifiés.



Paramètres du Dr.Web Cloud

Sur l'onglet **Dr.Web Cloud** vous pouvez autoriser ou interdire à **Dr.Web pour Linux** l'utilisation du service **Dr.Web Cloud**.

Dr.Web Cloud permet a la protection antivirus d'utiliser des informations actuelles sur les menaces, ces informations sont mises a jour sur les serveurs de **Doctor Web** en temps reel. En fonction des parametres de mises a jour, les informations sur les menaces utilisees par les composants de la protection antivirus peuvent etre obsoletes. Les services **Dr.Web Cloud** peuvent, de facon fiable, restreindre l'acces des utilisateurs de votre ordinateur aux sites de contenu non desirable ainsi que proteger contre les fichiers contamines.

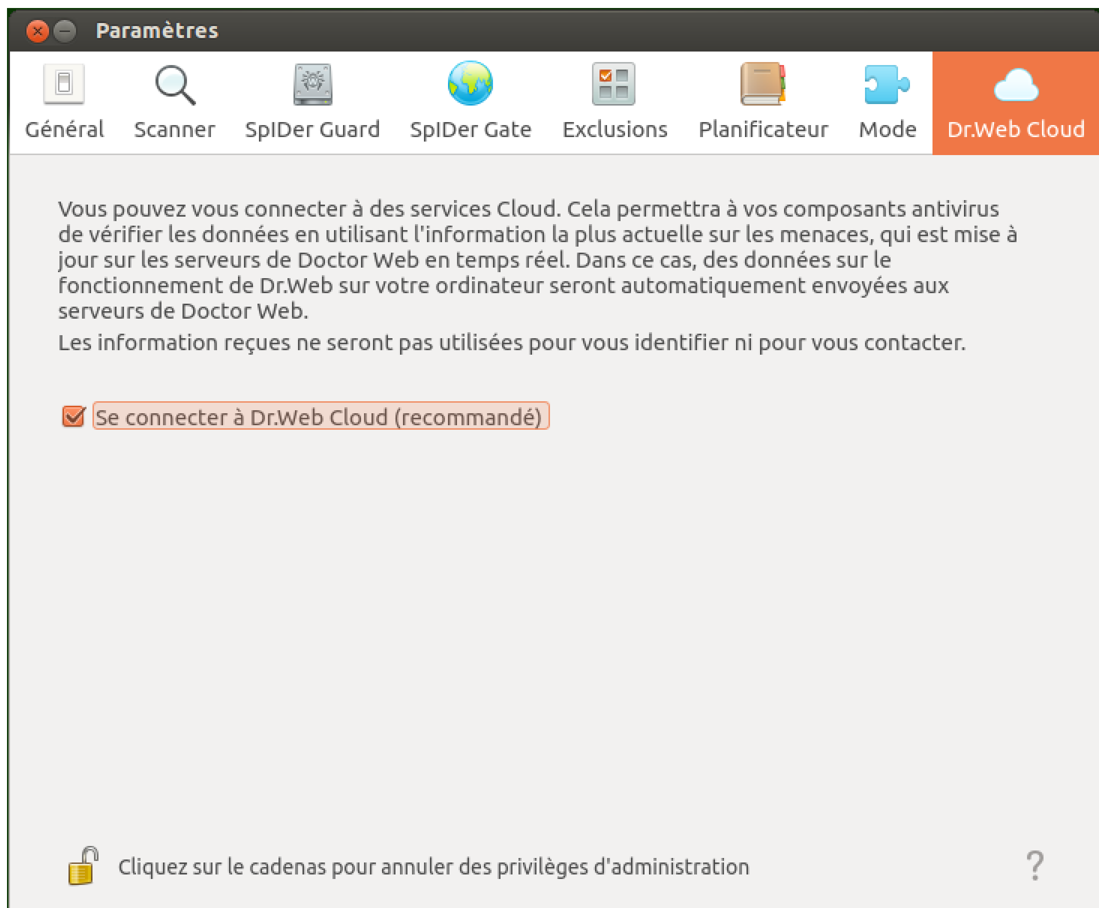


Image 65. Onglet Dr.Web Cloud

Pour autoriser ou interdire à **Dr.Web pour Linux** l'utilisation du service **Dr.Web Cloud**, cochez la case correspondante.



Pour accéder au service **Dr.Web Cloud** la connexion Internet est requise.

Pour autoriser ou interdire à **Dr.Web pour Linux** l'utilisation du service **Dr.Web Cloud**, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gérer les Privilèges du Logiciel.



Avancé

Paramètres en Ligne de Commande

Pour démarrer **Dr.Web pour Linux** en mode graphique depuis la ligne de commande, la commande suivante est utilisée:

```
$ drweb-gui [options]
```

Vous pouvez indiquer les options de commande suivantes:

Short case	Full case	Arguments
-h	--help	
Description: Afficher les informations sur la commande supportée – ligne de paramètres et sortir		
-v	--version	
Description: Afficher les informations sur la version du module et sortir		

Exemple

```
$ drweb-gui --help
```

Cette commande affiche une courte information sur les paramètres en ligne de commande de l’interface graphique **Dr.Web pour Linux**.

Travailler en ligne de commande

Vous pouvez gérer le fonctionnement de **Dr.Web pour Linux** en ligne de commande à l’aide d’un outil spécifique- **drweb-ctl**.

Vous pouvez effectuer les actions suivantes en ligne de commande:

- Lancer le scan des objets du système de fichiers y compris les secteurs d’amorçage
- Lancer la mise à jour des bases virales
- Voir et modifier les paramètres de configuration de **Dr.Web pour Linux**
- Voir le statut des composants de **Dr.Web pour Linux** et les statistiques sur les menaces détectées
- Voir la quarantaine et gérer les objets placés en quarantaine
- Vous connecter ou vous déconnecter du serveur de protection centralisée

Les commandes utilisateur pour la gestion de **Dr.Web pour Linux** ont un effet seulement si les composants de **Dr.Web pour Linux** sont en cours d’exécution (par défaut, ils sont automatiquement lances au démarrage du système).



Notez que certaines commandes de contrôle requièrent les privilèges de superuser.
Pour élever les privilèges, utilisez la commande **su** (modifier l’utilisateur en cours) ou la commande **sudo** (exécuter la commande indiquée avec les privilèges d’un autre utilisateur).

L’outil **drweb-ctl** supporte la saisie semi-automatique des commandes de gestion de **Dr.Web pour Linux** si cette option est activée dans l’interface de commande utilisée. Si l’interface de commande n’autorise pas la saisie semi-automatique, vous pouvez configurer cette option. Pour cela, référez-vous au manuel d’instructions correspondant à la distribution du système d’exploitation utilisé.



Format d’appel

1. Format d’appel de l’utilitaire

Le format d’appel pour l’outil de la ligne de commande qui gère **Dr.Web pour Linux** se présente comme suit :

```
$ drweb-ctl [<general options> | <command> [<argument>] [<command options>]]
```

où :

- `<general options>` – options qui peuvent être appliquées au démarrage lorsque la commande n’est pas spécifiée ou à n’importe quelle commande. Non obligatoire pour le démarrage.
- **`<command>`** – commande devant être effectuée par **Dr.Web pour Linux** (par exemple, démarrage du scan, sortie de la liste des objets en quarantaine).
- `<argument>` – argument de commande. Dépend de la commande indiquée. Peut être absent pour certaines commandes.
- `<command options>` – options gérant le fonctionnement de la commande. Dépend de la commande. Peut être absent pour certaines commandes.

2. Options générales

Les options générales suivantes sont disponibles :

Option	Description
`-h`, `--help`	Afficher les informations d’aide résumées et sortir. Pour des informations sur une commande en particulier, entrez la ligne suivante : **`drweb-ctl`** `-h` **`<command>`** ou **`drweb-ctl`** **`<command>`** `-h`
`-v`, `--version`	Afficher les informations sur la version du module et sortir
`-d`, `--debug`	Indique d’afficher les informations de débogage après l’exécution de la commande spécifiée. Cela n’a pas d’effet si une commande n’est pas spécifiée Pour appeler une commande, entrez la ligne suivante: **`drweb-ctl`** `-d` **`<command>`**

3. Commandes

Les commandes de gestion de **Dr.Web pour Linux** peuvent être divisées en groupes :

- Commandes de scan antivirus
- Commandes pour gérer les mises à jour et le fonctionnement en *mode Protection centralisée*
- Commandes de gestion de la configuration
- Commandes pour gérer les menaces détectées et la quarantaine
- Commandes d’affichage d’informations



3.1. Commandes de scan antivirus

Les commandes suivantes pour gérer le scan antivirus sont disponibles :

Commande	Description
scan <path>	**Fonctionnalité** Lancer un contrôle du fichier ou du répertoire spécifiés par le **Scanner**. **Arguments** <path> – Chemin vers le fichier ou le répertoire sélectionné pour être scanné. Cet argument peut être absent si l'option --stdin ou --stdin0 est activée. Pour indiquer plusieurs fichiers satisfaisant à certains critères, utilisez l'utilitaire **find** (voir les exemples) et les options --stdin ou --stdin0. **Options** -a [--Autonomous] – Lance une instance séparée du moteur **Dr.Web pour Linux** et du **Scanner** et les arrête après la fin des tâches de scan. Notez que les menaces détectées durant un scan automatique ne sont pas affichées dans la liste commune des menaces qui est émise par la commande menaces (voir ci-dessous). --stdin – Obtenir la liste des chemins à scanner depuis la chaîne de saisie standard (stdin). Les chemins dans la liste doivent être séparés par la nouvelle ligne de caractères('\n'). --stdin0 – Obtenir la liste des chemins à scanner depuis la chaîne de saisie standard (stdin). Les chemins dans la liste doivent être séparés par le caractère NUL ('\0'). Notez que les modèles ne sont pas autorisés lorsque des chemins sont indiqués pour chacune des options. L'utilisation recommandée des options --stdin et --stdin0 est de générer une liste de chemins (générée par un utilitaire externe, par exemple **find**), dans la commande **scan** (voir les exemples). --Report <BRIEF|DEBUG> – Indiquer le type de rapport pour les résultats de scan. Valeurs possibles : • BRIEF – rapport court. • DEBUG – rapport détaillé. Valeur par défaut : BRIEF --ScanTimeout <number> – Indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à 0, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut : 0 --PackerMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan d'objets empaquetés. Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : 8 --ArchiveMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan des archives (zip, rar, etc.). Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : 8 --MailMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan d'email (pst, tbb, etc.). Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés.



Commande	Description
	Valeur par défaut : 8 --ContainerMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan de conteneurs d'un autre type (HTML et autres). Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : 8 --MaxCompressionRatio <ratio> – Indiquer le ratio de compression maximum pour les objets scannés. Le ratio doit être au moins égal à 2. Valeur par défaut : 3000 --HeuristicAnalysis <On|Off> – Activer ou désactiver *l'analyse heuristique*. Valeur par défaut : On --OnKnownVirus <action> – Action appliquée à une menace détectée en utilisant l'analyse par signatures. Valeurs autorisées : REPORT, CURE, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnIncurable <action> – Action appliquée en cas d'échec de traitement d'une menace détectée ou si la menace est incurable. Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnSuspicious <action> – Action appliquée à une menace détectée en utilisant l'analyse heuristique. Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnAdware <action> – Action appliquée aux adwares. Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnDialers <action> – Action appliquée aux dialers. Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnJokes <action> – Action appliquée aux canulars Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnRiskware <action> – Action appliquée à un programme potentiellement dangereux (riskware). Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT --OnHacktools <action> – Action appliquée à un hacktool. Valeurs autorisées : REPORT, QUARANTINE, DELETE. Valeur par défaut : REPORT
bootscan <disk drive> | ALL	**Fonctionnalité** Démarrer le scan des secteurs d'amorçage sur les disques indiqués avec le **Scanner**. Les secteurs MBR et VBR sont scannés. **Arguments**



Commande	Description
	`<disk drive>` – Chemin vers un fichier bloc du disque dont le secteur d'amorçage doit être scanné. Si vous indiquez la valeur `ALL`, tous les secteurs d'amorçage de tous les disques disponibles seront scannés. Argument obligatoire. **Options** `-a [--Autonomous]` – Démarre une instance séparée du moteur **Dr.Web pour Linux** et du **Scanner** et les arrête après la fin des tâches de scan. Notez que les menaces détectées durant un scan automatique ne sont pas affichées dans la liste commune des menaces qui est émise par la commande `menaces` (voir ci-dessous). `--Report <BRIEF|DEBUG>` – Indiquer le type de rapport pour les résultats de scan. Valeurs possibles : • `BRIEF` – rapport court. • `DEBUG` – rapport détaillé. Valeur par défaut : `BRIEF` `--ScanTimeout <number>` – Indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à 0, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut : 0 `--HeuristicAnalysis <On|Off>` – Activer ou désactiver *l'analyse heuristique*. Valeur par défaut : `On` `--Cure <Yes|No>` – Activer ou désactiver les tentatives de réparation des menaces détectées. Si la valeur est égale à `No`, seule la notification est émise. Valeur par défaut : `No` `--ShellTrace` – Activer l'émission d'informations de débogage supplémentaires lors du scan du secteur d'amorçage.
procscan	**Fonctionnalité** Démarrer le contrôle des fichiers exécutables contenant le code des processus en cours d'exécution avec le **Scanner**. **Arguments** Non. **Options** `-a [--Autonomous]` – Démarre une instance séparée du moteur **Dr.Web pour Linux** et du **Scanner** et les arrête après la fin des tâches de scan. Notez que les menaces détectées durant un scan automatique ne sont pas affichées dans la liste commune des menaces qui est émise par la commande `menaces` (voir ci-dessous). `--Report <BRIEF|DEBUG>` – Indiquer le type de rapport pour les résultats de scan. Valeurs autorisées : • `BRIEF` – rapport court. • `DEBUG` – rapport détaillé. Valeur par défaut : `BRIEF` `--ScanTimeout <number>` – Indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à 0, la durée de scan d'un fichier n'est pas limitée.



Commande	Description
	Valeur par défaut : 0 `--HeuristicAnalysis <On|Off>` – Activer ou désactiver *l'analyse heuristique*. Valeur par défaut : `On` `--PackerMaxLevel <number>` – Indiquer le niveau d'emboîtement maximum lors du scan d'objets empaquetés. Si la valeur est égale à `0`, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : `8` `--OnKnownVirus <action>` – Action appliquée à une menace détectée en utilisant l'analyse par signatures. Valeurs autorisées : `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnIncurable <action>` – Action appliquée en cas d'échec de traitement d'une menace détectée ou si la menace est incurable. Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnSuspicious <action>` – Action appliquée à une menace détectée en utilisant l'analyse heuristique. Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnAdware <action>` – Action appliquée aux adwares. Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnDialers <action>` – Action appliquée aux dialers. Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnJokes <action>` – Action appliquée aux canulars. Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnRiskware <action>` – Action appliquée aux programmes potentiellement dangereux (riskwares). Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` `--OnHacktools <action>` – Action appliquée aux hacktools. Valeurs autorisées : `REPORT`, `QUARANTINE`, `DELETE`. Valeur par défaut : `REPORT` Notez que si une menace est détectée dans un fichier exécutable, **Dr.Web pour Linux** arrête tous les processus lancés par le fichier.
`cloudscan`	**Fonctionnalité** Commencer l'analyse du fichier ou le répertoire indiqué par la connexion au service **Dr.Web Cloud** afin d'obtenir les informations sur la nocivité de ce fichier. **Arguments** `<path>` – chemin vers le fichier ou le répertoire à analyser. **Options** `--Report <BRIEF|DEBUG>` – spécifier le type de rapport du scan.



Commande	Description
	Valeurs autorisées : • BRIEF – rapport court. • DEBUG – rapport détaillé. Valeur par défaut : BRIEF --ScanTimeout <number> – Indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à 0, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut : 0 --PackerMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan d'objets empaquetés. Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés.. Valeur par défaut : 8 --ArchiveMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan des archives (zip, rar, etc.). Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : 8 --MailMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan d'email (pst, tbb, etc.). Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : 8 --ContainerMaxLevel <number> – Indiquer le niveau d'emboîtement maximum lors du scan de conteneurs d'un autre type (HTML et autres). Si la valeur est égale à 0, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : 8 --MaxCompressionRatio <ratio> – Indiquer le ratio de compression maximum pour les objets scannés. Le ratio doit être au moins égal à 2 Valeur par défaut : 3000 --HeuristicAnalysis <On|Off> – *Activer ou désactiver l'analyse heuristique.* Valeur par défaut : On --Cure <Yes|No> – Activer ou désactiver les tentatives de réparation des menaces détectées. Si la valeur est égale à No, seule la notification est émise. Valeur par défaut : No --ShellTrace – Activer l'émission d'informations de débogage supplémentaires lors du scan du fichier.

3.2. Commandes pour gérer les mises à jour et le fonctionnement en mode Protection centralisée

Les commandes suivantes pour la gestion des mises à jour et le fonctionnement en mode Protection centralisée sont disponibles :

Commande	Description
`update`	**Fonctionnalité** Indique à **l'Updater** de télécharger et d'installer les mises à jour des bases virales et des composants depuis les serveurs de mise à jour de **Doctor Web** ou de terminer un processus de mise à jour en cours.



Commande	Description
	La commande n’a pas d’effet si **Dr.Web pour Linux** est connecté au serveur de protection centralisée. **Arguments** Non. **Options** `--Stop` – Terminer le processus de mise à jour en cours.
`esconnect` `<server>[:port]`	**Fonctionnalité** Connecter **Dr.Web pour Linux** au serveur de protection centralisée spécifié (par exemple, le Serveur Entreprise **Dr.Web**). Pour en savoir plus sur les modes opératoires de l’Antivirus, consultez la section Modes opératoires. **Arguments** • `<server>` – Adresse IP ou nom réseau de l’hôte sur lequel le serveur de protection centralisée fonctionne. L’argument est obligatoire. • `<port>` – Nom du port utilisé par le serveur de protection centralisée. L’argument est optionnel. Indiquez l’argument uniquement si le serveur de protection centralisée utilise un port non standard. **Options** `--Key <path>` – Chemin vers le fichier de la clé publique du serveur de protection centralisée auquel **Dr.Web pour Linux** est connecté. `--Login <ID>` – Login (identificateur du poste de travail) utilisé pour la connexion au serveur de protection centralisée. `--Password <password>` – Mot de passe pour la connexion au serveur de protection centralisée. `--Group <ID>` – Identificateur du groupe auquel le poste de travail est relié lors de la connexion. `--Rate <ID>` – Identificateur du groupe de tarif appliqué à un poste de travail lorsqu’il est inclus à l’un des groupes du serveur de protection centralisée (peut être indiqué uniquement en même temps que l’option `--Group`). `--Compress <On|Off>` – Active (`On`) ou désactive (`Off`) la compression forcée des données transmises. Lorsque rien n’est indiqué, l’utilisation de la compression est déterminée par le serveur. `--Encrypt <On|Off>` – Active (`On`) ou désactive (`Off`) le chiffrement forcé des données transmises. Lorsque rien n’est indiqué, le chiffrement est déterminé par le serveur. `--Newbie` – Connecter comme “novice” (obtenir un nouveau compte sur le serveur). `--WithoutKey` – Autorise la connexion au serveur sans utiliser de clé publique. `--WrongKey` – Autorise la connexion au serveur même si la clé publique indiquée n’est pas correcte. Les options `--Key` and `--WithoutKey` sont réciproquement exclusives. Une de ces options doit être indiquée dans la commande. Notez que cette commande demande que **`drweb-ctl`** soit lancé avec les privilèges de superuser.
`esdisconnect`	**Fonctionnalité** Déconnecter **Dr.Web pour Linux** du serveur de protection centralisée et passer en mode autonome. La commande n’a pas d’effet si **Dr.Web pour Linux** est en mode autonome. **Arguments**



Commande	Description
	Non. **Options** Non. Notez que cette commande demande que **drweb-ctl** soit lancé avec les privilèges de superuser.

3.3. Commandes de gestion de la configuration

Les commandes suivantes pour gérer la configuration sont disponibles :

Commande	Description
cfset `<section>.<parameter> <value>`	**Fonctionnalité** Modifier la valeur active du paramètre indiqué dans la configuration actuelle. Notez que le signe égal n'est pas autorisé. **Arguments** • `<section>` – Nom du fichier de configuration où le paramètre réside. L'argument est obligatoire. • `<parameter>` – Nom du paramètre L'argument est obligatoire. • `<value>` – Nouvelle valeur devant être assignée au paramètre. L'argument est obligatoire. Le format suivant est utilisé pour indiquer la valeur du paramètre `<section>.<parameter> <value>` Pour une description du fichier de configuration, consultez le `man drweb.ini(5)`. **Options** `-a [--Add]` – Ne remplacez pas la valeur actuelle du paramètre mais ajoutez la valeur indiquée à la liste (autorisé uniquement pour les paramètres qui peuvent avoir plusieurs valeurs, indiqués dans une liste). `-e [--Erase]` – Ne remplacez pas la valeur actuelle du paramètre mais supprimez la valeur indiquée de la liste (autorisé uniquement pour les paramètres qui peuvent avoir plusieurs valeurs, indiqués dans une liste). `-r [--Reset]` – Restaurer la valeur du paramètre par défaut. Ainsi, `<value>` n'est pas requis dans la commande et est ignoré si indiqué. Les options ne sont pas obligatoires Si elles ne sont pas activées, la valeur actuelle du paramètre (ou la liste des valeurs si plusieurs sont indiquées) est remplacée par la valeur indiquée. Pour l'option `-r`, une syntaxe spéciale pour appeler la commande **cfset** est utilisée: **cfset** `<section>.* -r` Dans ce cas, tous les paramètres de la section spécifiée sont restaurés dans leurs valeurs par défaut. Notez que cette commande demande que **drweb-ctl** soit lancé avec les privilèges de superuser.
cfshow `[<section>][.<parameter>]`	**Fonctionnalité** Afficher les paramètres de la configuration actuelle. La commande pour afficher les paramètres se présente comme ceci `<section>.<parameter> = <value>`. Les sections et paramètres des composants qui ne sont pas installés ne sont pas affichés. **Arguments**



Commande	Description
	• `<section>` – Nom des paramètres de la section du fichier de configuration qui doivent être affichés. L'argument est optionnel. S'il n'est pas spécifié, les paramètres de toutes les sections du fichier de configuration sont affichés. • `<parameters>` – Nom du paramètre affiché. L'argument est optionnel. S'il n'est pas spécifié, tous les paramètres de la section sont affichés. Sinon, seul ce paramètre est affiché. Si un paramètre est indiqué sans le nom de la section, tous les paramètres portant ce nom pour toutes les sections du fichier de configuration sont affichés. **Options** `--Uncut` – Afficher tous les paramètres de configuration (et non seulement ceux utilisés avec l'ensemble des composants actuellement installés). Si l'option n'est pas spécifiée, seuls les paramètres utilisés pour la configuration des composants installés s'affichent `--Ini` – Afficher les valeurs du paramètre au format INI : tout d'abord, le nom de la section est indiqué entre crochets, puis les paramètres de la section sont listés par paires <parameter> = <value> (une paire par ligne).

3.4. Commandes pour gérer les menaces détectées et la quarantaine

Les commandes suivantes pour gérer les menaces détectées et la quarantaine sont disponibles :

Commande	Description
threats `[<command> <object>]`	**Fonctionnalité** Appliquer l'action spécifiée aux menaces détectées par leurs identificateurs. Le type d'action est configuré via l'option de commande indiquée. Si aucune action n'est spécifiée, des informations sur les menaces détectées sont affichées mais pas sur les menaces neutralisées. **Arguments** Non. **Options** `-f [--Follow]` – Attendre les nouveaux messages sur les nouvelles menaces et afficher les messages à leur réception (interrompre l'attente par **^C**). `--Cure <threat list>` – Essayer de traiter les menaces listées (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules). `--Quarantine <threat list>` – Déplacer les menaces listées en quarantaine (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules) `--Delete <threat list>` – Supprimer les menaces listées (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules). `--Ignore <threat list>` – Ignorer les menaces listées (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules). S'il est nécessaire d'appliquer la commande à toutes les menaces détectées, indiquez `all` au lieu de `<threat list>`. Par exemple, la commande suivante **`drweb-ctl`** `threats --Quarantine all` Déplace tous les objets malveillants détectés en quarantaine.
quarantine `[<command> <object>]`	**Fonctionnalité** Appliquer une action à l'objet indiqué en quarantaine. Si aucune action n'est appliquée, les informations suivantes s'affichent : identificateur des objets en quarantaine et courtes informations sur les fichiers source. **Arguments**



Commande	Description
	Non. **Options** `--Delete <object>` – Supprimer l’objet indiqué de la quarantaine. Notez que les objets sont supprimés définitivement de la quarantaine. `--Cure <object>` – Essayer de traiter l’objet indiqué en quarantaine. Notez que même en cas de désinfection, l'objet restera en quarantaine. Pour retirer l’objet désinfecté de la quarantaine appliquez la commande de restauration `--Restore`. `--Restore <object>` – Restaurer l’objet indiqué de la quarantaine vers sont emplacement d’origine. Notez que l’application de cette commande peut exiger le lancement de **`drweb-ctl`** par l’utilisateur root. L’objet peut être restauré de la quarantaine même s’il est infecté. Comme `<object>` indiquez l’identificateur de l’objet en quarantaine. Pour appliquer la commande à tous les objets placés en quarantaine, indiquez `all` comme `<object>`. Par exemple, la commande suivante **`drweb-ctl`** `quarantine --Restore all` Restaure tous les objets de la quarantaine.

3.5. Commandes d’affichage d’informations

Les commandes d’affichage d’informations suivantes sont disponibles :

Commande	Description
`appinfo`	**Fonctionnalité** Afficher des informations sur les modules actifs de **Dr.Web pour Linux**. **Arguments** Non. **Options** `-f [--Follow]` – Attendre les nouveaux messages sur le changement de statut du module et les afficher dès leur réception (interrompre l’attente par **`^C`**).
`baseinfo`	**Fonctionnalité** Afficher des informations sur la version actuelle du moteur **Dr.Web pour Linux** et le statut des bases virales. **Arguments** Non. **Options** Non.
`license`	**Fonctionnalité** Afficher des informations sur la licence active. **Arguments** Non. **Options** Non.



Exemple d'Utilisation

Exemple d'utilisation de la commande **drweb-ctl** :

1) Lancer le scan du répertoire `/home` avec les paramètres par défaut :

```
$ drweb-ctl scan /home
```

2) Chemins du scan listés dans le fichier `daily_scan` (un chemin par ligne) :

```
$ drweb-ctl scan --stdin < daily_scan
```

3) Lancer le scan du secteur d'amorçage du disque **sda** :

```
$ drweb-ctl bootscan /dev/sda
```

4) Afficher tous les paramètres de la configuration active depuis la section `[Root]` :

```
$ drweb-ctl cfshow Root
```

5) Indiquer `'No'` comme valeur du paramètre de **Démarrage** dans la section `[LinuxSpider]` (ce paramètre désactive **SpIDer Guard** – moniteur du système de fichiers dans l'OS **Linux** OS) :

```
# drweb-ctl cfset LinuxSpider.Start No
```

Notez que les privilèges de superuser sont requis pour effectuer cette action. Pour élever les privilèges, vous pouvez utiliser la commande **sudo**, comme dans l'exemple suivant :

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

Exemple d'utilisation de l'utilitaire **find** pour sélectionner des fichiers à scanner (la commande **drweb-ctl** `scan --stdin`) :

1) Scanner tous les fichiers dans tous les répertoires, en commençant par le répertoire racine, dans la même partition du système de fichiers :

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

2) Scanner tous les fichiers dans tous les répertoires, en commençant par le répertoire racine, exceptés les fichiers résidant dans les répertoires `/var/log/messages` et `/var/log/syslog` :

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog | drweb-ctl
scan -stdin
```

3) Scanner tous les fichiers de l'utilisateur `racine` dans tous les répertoires en commençant par le répertoire racine :

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

4) Scanner les fichiers de l'utilisateur `racine` et `admin` dans tous les répertoires, en commençant par le répertoire racine :

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

5) Scanner les fichiers des utilisateurs avec un `UID` dans la fourchette `1000 – 1005` dans tous les répertoires, en commençant par le répertoire racine :

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

6) Scanner les fichiers dans tous les répertoires en commençant par le répertoire racine avec un niveau d'emboîtement inférieur ou égal à 5 :

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```



7) Scanner les fichiers dans un répertoire racine en ignorant les fichiers dans les sous-répertoires :

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

8) Scanner les fichiers dans tous les répertoires en commençant par le répertoire racine en suivant tous les liens symboliques :

```
$ find -L / -type f | drweb-ctl scan --stdin
```

9) Scanner les fichiers dans tous les répertoires en commençant par le répertoire racine sans suivre les liens symboliques :

```
$ find -P / -type f | drweb-ctl scan --stdin
```

10) Scanner les fichiers créés au plus tard le 3 Juillet 2013 dans tous les répertoires en commençant par le répertoire racine :

```
$ find / -type f -newermt 2013-07-03 | drweb-ctl scan --stdin
```



Annexes

Annexe A. Types de menaces informatiques

Sous le terme « *menace* », nous entendons tout logiciel pouvant potentiellement ou directement endommager l'ordinateur ou le réseau, ou porter atteinte aux données ou aux droits de l'utilisateur (logiciels malveillants ou indésirables). Dans le sens le plus large du terme, « menace » peut indiquer tout type de danger potentiel pour la sécurité de l'ordinateur ou du réseau (ainsi, une vulnérabilité peut être utilisée pour des attaques de pirates).

Tous les types de logiciels décrits ci-dessous peuvent présenter un danger pour les données de l'utilisateur et pour son droit à la confidentialité. Les logiciels qui ne dissimulent pas leur présence dans le système (par exemple, certains logiciels pour diffusion de spam ou analyseurs du trafic), ne sont normalement pas considérés comme menaces, mais peuvent l'être sous certaines conditions.

Selon la classification de **Doctor Web**, toutes les menaces sont divisées en deux types, suivant le niveau de danger qu'elles représentent :

* **Menaces graves** – ce sont des menaces classiques qui sont capables de mener par elles-mêmes des actions destructives et illégales au sein du système (suppression et vol de données, défaillance du réseau etc.). Ce type de menace regroupe les logiciels appelés traditionnellement malwares (logiciels malveillants). Ce sont les vers, virus et Chevaux de Troie.
* **Menaces mineures** – ce sont des menaces considérées comme moins dangereuses mais qui pourraient être utilisées par une tierce personne pour effectuer des actions malveillantes. De plus, toute présence de menaces, même mineures, dans le système, témoigne de sa vulnérabilité. Les spécialistes de la sécurité informatique qualifient ce type de menaces de logiciels « gris » (grayware) ou de « logiciels potentiellement non-sollicités » (PUP –Potentially Unwanted Programs) qui sont des logiciels de types : adwares, dialers, canulars, riskwares et hacktools.

Menaces graves

Virus informatiques

Ce type de menaces informatiques se caractérise par sa capacité à introduire son code dans le code d'exécution d'autres logiciels. Cette pénétration porte le nom d'infection. Dans la plupart des cas, le fichier infecté devient lui-même porteur du virus et le code introduit n'est plus conforme à l'original. La majeure partie des virus est conçue pour détériorer ou détruire les données du système.

Dans la classification de **Doctor Web**, les virus sont catégorisés par le type d'objets qu'ils infectent :

* **Virus de fichier** - virus infectant les fichiers système (fichiers exécutables, bibliothèques dynamiques) et qui s'activent au lancement du fichier infecté ;
* **Macrovirus** infectant les fichiers utilisés par les applications Microsoft® Office et d'autres programmes utilisant des commandes macros (généralement écrits en Visual Basic). Les commandes macros sont des logiciels internes (macros), écrits dans un langage de programmation totalement fonctionnel. Par exemple, dans Microsoft® Word, les macros se lancent automatiquement lorsque vous ouvrez, (fermez, sauvegardez etc) un document.
* **Virus script** - virus écrits en langages de script qui infectent dans la plupart des cas d'autres scripts (par exemple, les fichiers du système d'exploitation). Ils peuvent également infecter d'autres formats de fichiers qui supportent l'exécution des scripts, tout en se servant des scripts vulnérables des applications Web ;



* **Virus de boot** - ils infectent les secteurs d’amorçage des disques et des partitions aussi bien que les principaux secteurs boot des disques durs. Ils occupent peu de mémoire et restent prêts à remplir leurs fonctions jusqu'à ce qu'un déchargement, un redémarrage ou un arrêt du système ne soient effectués.

La plupart des virus possèdent des mécanismes de protection contre leur détection. Leurs méthodes de protection contre la détection s'améliorent sans cesse, de même que les moyens pour les contrer. On peut également classer les virus selon le moyen de protection contre la détection qu’ils utilisent :

* **Virus chiffrés** - Ils chiffrent leur code à chaque infection afin de rendre leur détection dans un fichier, un secteur d’amorçage ou en mémoire, plus difficile. Toutes les variantes de ce type de virus contiennent uniquement un petit fragment de code en commun (la procédure de déchiffrement) qui peut être utilisé comme la signature du virus ;
* **Virus polymorphes** - ce sont des virus qui chiffrent également leur code mais qui, en plus, utilisent un algorithme de déchiffrement spécifique différent à chaque nouvelle variante du virus. Ceci implique que ces types de virus n’ont pas de signature virale ;
* **Virus furtifs** - ils agissent de telle façon qu'ils masquent leur activité et cachent leur présence dans les objets infectés. Ces virus captent les caractéristiques d’un objet avant de l'infecter et présentent ensuite ces caractéristiques « modèles » au scanner antivirus cherchant, lui, à dépister des fichiers modifiés.

On peut également classifier les virus d'après le langage de programmation dans lequel ils sont écrits (la plupart sont écrits en Assembleur, en langages de haut niveau de programmation et en langages scripts etc.) ainsi que selon les systèmes d'exploitation ciblés.

Vers informatiques

Récemment, les vers sont devenus plus fréquents que les virus ou d'autres programmes malveillants. Tout comme les virus, ils sont capables de s’auto répliquer et de diffuser leurs copies, mais n'affectent pas d’autres logiciels ni fichiers (ils n’ont pas besoin des fichiers host pour se répandre). Les vers pénètrent dans un ordinateur via un réseau mondial ou local (souvent via une pièce jointe dans un email) et ils envoient massivement leurs propres copies à d’autres ordinateurs du réseau. Au départ, pour se propager, les vers peuvent profiter des actions de l'utilisateur ou choisir le poste à attaquer de manière automatique.

Les vers ne sont pas forcément composés d'un seul fichier (le corps du ver). Plusieurs d'entre eux possèdent également une partie infectieuse (le shellcode), qui se charge dans la mémoire vive (RAM) de l'ordinateur puis télécharge le corps du ver sous forme de fichier exécutable via le réseau. Si seul le shellcode est présent dans le système, le ver peut être supprimé en redémarrant simplement l'ordinateur (et la mémoire vive est déchargée et remise à zéro). Mais aussitôt que le corps du ver entre dans le système, seul l'antivirus peut le désinfecter.

A cause de leur propagation intense, les vers peuvent paralyser des réseaux entiers, même s'ils n'endommagent pas directement le système.

Doctor Web classifie les vers d'après leur mode de propagation :

* Les vers de réseau se propagent à l'aide de différents protocoles réseau ou d'échanges de fichiers ;
* Les vers de courrier se propagent via les protocoles de courrier électronique (POP3, SMTP, etc.) ;
* Les vers de tchat se propagent en utilisant les messageries instantanées (ICQ, IM, IRC etc.).

Chevaux de Troie (Trojans)

Ce type de logiciels malicieux n'est pas capable de s'auto répliquer ni d’infecter d’autres logiciels. Les Chevaux de Troie se substituent à des programmes très utilisés, effectuent les mêmes actions qu’eux ou en imitent le fonctionnement. Dans le même temps, ils effectuent des actions malveillantes dans le système (suppriment ou endommagent des fichiers ou des données, envoient les données confidentielles de l’utilisateur) ou donnent aux pirates un accès à l’ordinateur pour, par exemple, porter atteinte au propriétaire de l'ordinateur touché.



Les capacités de camouflage et d'endommagement d'un Cheval de Troie sont les mêmes que celles d'un virus. Un Trojan peut représenter lui-même un module de virus. Mais dans la plupart des cas, les Trojans se diffusent comme des fichiers exécutables isolés (via les serveurs d'échange de fichiers, les supports amovibles ou dans les pièces jointes des emails) qui sont exécutés par l'utilisateur lui-même ou par les tâches système.

Il est difficile de classifier les Trojans car ils sont souvent diffusés par des virus ou des vers mais également parce que beaucoup d'actions malveillantes pouvant être effectuées par d'autres types de menaces sont imputées aux Trojans uniquement. Certains types de trojans sont classés à part par les spécialistes de **Doctor Web** :

- **Backdoors** – ce sont des trojans qui offrent un accès privilégié au système, contournant le mécanisme existant d'accès et de protection. Les backdoors n'infectent pas les fichiers, mais ils s'inscrivent dans le registre, modifiant les clés de registre ;
- **Rootkits** – ils sont destinés à intercepter les fonctions de l'API du système d'exploitation pour dissimuler leur présence dans le système. En outre, le rootkit peut masquer les processus d'autres logiciels (par ex, d'autres menaces), les clés de registre, des fichiers et des dossiers. Le rootkit se propage comme un logiciel indépendant ou comme le composant d'un autre logiciel malveillant. Selon leur mode de fonctionnement, il existe deux types de rootkits : User Mode Rootkits (UMR) - qui fonctionnent dans le mode utilisateur (interception des fonctions des bibliothèques du mode utilisateur), et Kernel Mode Rootkits (KMR) - qui fonctionnent dans le mode noyau (interception des fonctions au niveau du noyau système, ce qui rend la détection plus difficile) ;
- **Keyloggers** – utilisés pour enregistrer les données entrées par l'utilisateur sur le clavier. Le but de ces actions est le vol des données personnelles (mots de passe, logins, numéros de cartes bancaires etc.) ;
- **Cliqueurs** – ils redirigent les liens quand on clique sur eux. D'ordinaire, l'utilisateur est redirigé vers des adresses déterminées avec le but d'augmenter le trafic publicitaire des sites web ou pour organiser des attaques DDoS ;
- **Trojans proxy** – ils offrent aux pirates un accès anonyme à Internet via l'ordinateur de leur victime.

Les Trojans peuvent accomplir d'autres actions malveillantes comme, par exemple, changer la page d'accueil du navigateur web de la victime ou supprimer certains fichiers. Mais ces actions peuvent également être exécutées par d'autres logiciels malicieux (virus et vers).

Menaces mineures

Hacktools

Les hacktools sont édités pour aider les hackers. Les logiciels de ce type les plus répandus sont des scanners de ports, sachant détecter les vulnérabilités des pare-feux (firewalls) et d'autres composants qui assurent la sécurité du système de l'ordinateur. A part les pirates, les administrateurs peuvent utiliser ce type d'outils pour vérifier la sécurité de leurs réseaux. Certains logiciels utilisés pour le hacking ou qui utilisent l'ingénierie sociale sont désignés comme des hacktools.

Adwares

Sous ce terme, on désigne le plus souvent un code interne aux logiciels gratuits qui impose l'affichage d'une publicité sur l'ordinateur de l'utilisateur. Mais parfois, ce code peut être diffusé par d'autres logiciels malveillants et afficher des publicités dans les navigateurs web. Très souvent, ces logiciels publicitaires fonctionnent en utilisant des données collectées par des logiciels espions.

Canulars

Ce type de logiciels malveillants, comme les logiciels publicitaires, ne détériorent pas le système. Ils génèrent le plus souvent des messages sur des erreurs inexistantes et effraient l'utilisateur pour effectuer des actions qui peuvent mener à la perte de données. Leur but est d'intimider l'utilisateur ou de l'irriter.



Dialers

Ce sont de petites applications installées sur les ordinateurs, élaborées spécialement pour scanner un certain spectre de numéros de téléphone. Par la suite, les malfaiteurs utiliseront les numéros trouvés pour prélever de l'argent à leur victime ou pour connecter l'utilisateur à des services téléphoniques surtaxés et coûteux.

Riskwares

Ces logiciels ne sont pas créés pour détériorer le système, mais peuvent être utilisés pour paralyser la sécurité du système grâce à certaines fonctionnalités. C'est pourquoi ils sont classés parmi les menaces mineures. Ces logiciels peuvent non seulement détériorer les données ou les supprimer par hasard, mais ils peuvent également être utilisés par des crackers ou par d'autres logiciels pirates pour nuire au système. Parmi ce type de logiciels, on peut trouver les tchat et les outils d'administration à distance, les serveurs FTP etc.

Objets suspects

Ce sont des menaces potentielles dépistées à l'aide de l'analyseur heuristique. Ces objets peuvent s'avérer appartenir à un des types de menaces informatiques (même encore inconnues) ou être absolument inoffensifs, en cas de faux positif.

Dans tous les cas, les objets suspects doivent être envoyés pour analyse au **Laboratoire viral de Doctor Web**.



Annexe B. Neutralisation des menaces

Toutes les solutions antivirus créées par **Dr.Web** utilisent un ensemble de méthodes de détection, ce qui leur permet d'effectuer des analyses en profondeur des fichiers suspects et de contrôler le comportement des logiciels.

Méthode de détection des menaces

Analyse par signature

Les scans commencent par *l'analyse par signature*, effectuée en comparant des segments de code de fichiers aux signatures des virus connus. Une *Signature* est une séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace. Pour réduire la taille de la base de signatures, les solutions Antivirus **Dr.Web** utilisent des sommes de contrôle de signatures au lieu de séquences complètes de signatures. Les sommes de contrôle identifient les signatures de manière unique, ce qui garantit l'exactitude de la détection de virus et leur neutralisation. Les bases de données virales de **Dr.Web** sont faites de telle sorte que certaines entrées peuvent être utilisées pour détecter non seulement un virus, mais une famille entière de menaces.

Origins Tracing

En complément de l'analyse par signature, les solutions Antivirus **Dr.Web** utilisent la méthode unique **Origins Tracing™** pour détecter de nouveaux virus ou des virus modifiés utilisant des mécanismes d'infection connus. Grâce à cette technologie, les utilisateurs de **Dr.Web** sont protégés contre des menaces telles que le **`Trojan.Encoder.18`** (également connu sous le nom «**`gpcode`**»). En outre, l'utilisation de la technologie **Origins Tracing™** peut réduire considérablement le nombre de faux positifs de l'analyseur heuristique. Les objets détectés grâce à l'algorithme **Origins Tracing™** sont indiqués avec l'extension `.Origin`.

Émulation d'exécution

La méthode d'émulation d'exécution de code est utilisée pour détecter les virus polymorphes et cryptés si la recherche à l'aide des sommes de contrôle des signatures est inapplicable ou considérablement compliquée en raison de l'impossibilité de construire des signatures fiables. La méthode consiste à simuler l'exécution du code en utilisant un *émulateur* – un modèle de programmation du processeur et de l'environnement d'exécution. L'Émulateur fonctionne avec un espace mémoire protégé (*tampon d'émulation*), dans lequel l'exécution du logiciel analysé est modélisée instruction par instruction. Cependant, les instructions ne sont pas transmises à un processeur central (CPU) pour exécution réelle. Lorsque l'émulateur reçoit un fichier infecté par un virus polymorphe, le résultat de l'émulation donne le corps décrypté du virus, qui est ensuite facilement trouvable via une recherche par les sommes de contrôles de signatures .

Analyse heuristique

Le fonctionnement de l'analyseur heuristique est fondé sur un ensemble d'*heuristiques* (hypothèses, dont la signification statistique est confirmée par l'expérience) sur les signes caractéristiques des codes malveillants et, inversement, sur les caractéristiques qui sont extrêmement rares dans les virus. Chaque attribut ou caractéristique du code possède un score indiquant le niveau de dangerosité et de fiabilité. Le score peut être positif si le signe indique la présence d'un comportement de code malveillant, et négatif si le signe ne correspond pas à une menace informatique. En fonction du score total du fichier, l'analyseur heuristique calcule la probabilité de la présence d'un objet malveillant inconnu. Si cette probabilité dépasse une certaine valeur de seuil, l'objet analysé est considéré comme malveillant.

L'analyseur heuristique utilise également la technologie **FLY-CODE ™** – un algorithme universel pour l'extraction des fichiers. Ce mécanisme permet de construire des hypothèses heuristiques sur la présence d'objets malveillants dans les objets, de logiciels compressés par des outils de compression (emballeurs), non seulement par des outils connus des développeurs des produits **Dr.Web**, mais également par des outils de compression nouveaux et inexplorés. Lors du contrôle des objets emballés, les solutions antivirus **Dr.Web** utilisent également l'analyse par entropie structurale. La technologie



détecte les menaces en assemblant des parties de code ; ainsi, une entrée dans la base de données permet l'identification de plusieurs menaces emballées par le même emballeur polymorphe.

Comme tout système basé sur des hypothèses, l'analyseur heuristique peut commettre des erreurs de type I ou II (omettre une menace ou faire un faux positif). Par conséquent, les objets détectés par l'analyseur heuristique reçoivent le statut «suspects».

Au cours de toute analyse, tous les composants des produits antivirus **Dr.Web** utilisent l'information la plus récente sur tous les programmes malveillants connus. Dès que les chasseurs de virus du **Laboratoire Viral Doctor Web** découvrent une nouvelle menace, une mise à jour de la base de données virales et des caractéristiques comportementales est publiée. Parfois, les mises à jour sont publiées plusieurs fois par heure. Ainsi, même si un virus passe au travers des gardiens résidents de **Dr.Web** et pénètre dans le système, il sera détecté après la mise à jour et neutralisé.

Actions

Les produits **Dr.Web** peuvent appliquer des actions spécifiques aux objets détectés pour neutraliser les menaces informatiques. L'utilisateur peut laisser le logiciel appliquer automatiquement les actions paramétrées par défaut, indiquer les actions à appliquer automatiquement, ou choisir manuellement une action spécifique pour chaque objet dépisté. Les actions disponibles sont :

- **Désinfecter** – s'applique aux menaces très importantes (virus, vers et trojans). Elle sous-entend une élimination du code nocif des fichiers contaminés et, dans la mesure du possible, la restauration des fichiers contaminés dans leur état initial « sain ». Certains fichiers contaminés ne se composent que d'un code malveillant (Trojans ou copies fonctionnelles des vers), ils doivent donc être supprimés entièrement. Tous les fichiers contaminés ne peuvent pas être désinfectés, mais les algorithmes de désinfection se perfectionnent sans cesse.
- **Quarantaine** (**Déplacer en quarantaine**) permet de déplacer une menace dans un dossier spécial et de l'isoler du reste du système. Cette action doit être appliquée lorsqu'aucun traitement n'est possible ou bien s'il s'agit d'objets suspects. Il est recommandé d'envoyer des copies de ces fichiers au **Laboratoire Viral de Doctor Web** afin qu'il les analyse.
- **Supprimer** est le procédé le plus radical appliqué aux menaces de tous types. Cette action peut être appliquée à tout type de menace. Elle sera parfois appliquée à un objet pour lequel l'action "Désinfecter" avait été préalablement choisie. Ceci peut se produire si l'objet infecté ne représente qu'un code malveillant et ne contient pas d'information utile (par exemple, le traitement d'un ver informatique implique la suppression de toutes ses copies fonctionnelles).
- **Ignorer** – action appliquée aux menaces mineures uniquement (pop-up publicitaires, dialers, canulars, logiciels potentiellement dangereux et hacktools), qui indique de passer la menace sans lui appliquer d'action ni afficher d'information sur sa nature.
- **Rapport** – lorsqu'aucune action n'est appliquée à un objet, les informations le concernant sont néanmoins affichées dans le tableau des résultats du scan.



Annexe C. Contacter le Support technique

Si vous avez des problèmes avec l'installation ou le fonctionnement des produits de notre société, différentes options de support sont disponibles :

- Télécharger les dernières versions des manuels et des guides à la page http://download.drweb.fr/;
- Consulter la rubrique des questions fréquentes http://support.drweb.fr/;
- Aller sur le **Forum officiel de Dr.Web** à la page http://forum.drweb.com/

Si vous n'avez pas trouvé de solution à votre problème, vous pouvez demander une assistance du **Support Technique de Doctor Web** en remplissant le formulaire sur la page correspondante de notre site : http://support.drweb.fr/support_wizard.

Pour en savoir plus sur les bureaux régionaux, visitez le site officiel de **Doctor Web** à la page http://company.drweb.fr/contacts/offices/.



Annexe D. Erreurs connues



Si vous ne trouvez pas la description de l'erreur survenue, il est recommandé de contacter le Support technique. Il vous sera demandé de donner le code d'erreur et de décrire les étapes qui y ont conduit afin de reproduire le problème.

Erreurs, déterminées par le code

Message d'erreur : *Fonctionnalité non implémentée.*

Code d'erreur : `x65`

Description : Un des composants de **Dr.Web pour Linux** peut ne pas fonctionner car il est nécessaire pour exécuter une fonctionnalité qui n'est pas implémentée dans la version actuelle.

Résoudre l'erreur :

SpIDer Gate : tentative d'activer le contrôle des connexions entrantes.

- Exécutez la commande

  ```
  # drweb-ctl cfset GateD.InputDivert Off
  ```

  Pour désactiver le contrôle des connexions entrants par **SpIDer Gate**.

Autres composants :

- Restaurer les paramètres par défaut du logiciel. Pour cela
  1. Effacez les contenus du fichier `/etc/opt/drweb.com/drweb.ini`. Il est recommandé de faire une copie de sauvegarde du fichier avant la procédure. Par exemple :

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

  2. Exécutez la commande

     ```
     # service drweb-configd restart
     ```

     Pour redémarrer **Dr.Web pour Linux**.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Fichier DRL invalide.*

Code d'erreur : `x90`

Description : La mise à jour ne peut pas être effectuée si **l'Updater** a détecté une violation de l'intégrité du logiciel ou s'il ne trouve pas de fichier signé avec la liste des serveurs de mise à jour.

Résoudre l'erreur :

- Installez les `drweb-bases` et les composants (packages) `drweb-dws` séparément puis lancez une mise à jour.
- Si l'erreur persiste, supprimez **Dr.Web pour Linux** puis réinstallez-le et relancez la mise à jour.
- Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.



Message d’erreur : *Fichier compressé invalide.*

Code d'erreur : `x92`

Description : **l’Updater** a détecté une violation de l’intégrité du logiciel ou ne trouve pas le fichier archive reçu du serveur de mise à jour.

Résoudre l’erreur :

- Relancez la mise à jour après une durée déterminée.

Si l’erreur persiste, contactez le Support technique et indiquez le code d’erreur.

Message d’erreur : *Erreur d’authentification sur le proxy.*

Code d'erreur : `x93`

Description : **l’Updater** n’a pas pu se connecter à un serveur de mise à jour car il n’est pas authentifié sur le serveur proxy utilisé pour recevoir les mises à jour.

Résoudre l’erreur :

- Vérifiez et corrigez les paramètres du serveur proxy utilisé (nom d’utilisateur et mot de passe utilisé pour l’authentification).
- Si l’erreur persiste, changez de serveur proxy ou n’utilisez pas de proxy pour les connexions.

Si l’erreur persiste, contactez le Support technique et indiquez le code d’erreur.

Message d’erreur : *Aucun serveur de mise à jour disponible.*

Code d'erreur : `x94`

Description : **l’Updater** ne peut se connecter à aucun serveur de mise à jour.

Résoudre l’erreur :

- Vérifiez que la connexion réseau est établie et vérifiez la connectivité. Assurez-vous que votre ordinateur est connecté à Internet.
- Si la connexion Internet n’est autorisée que via le proxy, configurez l’utilisation du proxy pour recevoir les mises à jour.
- Si un serveur proxy est utilisé, vérifiez et configurez les paramètres de connexion.

Si l’erreur persiste, contactez le Support technique et indiquez le code d’erreur.

Message d’erreur : *Le format de fichier est inconnu ou non supporté.*

Code d'erreur : `x95`

Description : Les mises à jour ne peuvent pas être reçues car l’intégrité du fichier clé a été violée.

Résoudre l’erreur :

- Installez le fichier clé depuis la copie de sauvegarde. Si vous ne trouvez pas la copie de sauvegarde, contactez le support technique pour l’obtenir.

Si l’erreur persiste, contactez le Support technique et indiquez le code d’erreur.

Message d’erreur : *La licence a déjà expiré.*



Code d'erreur : `x96`

Description : Les mises à jour ne peuvent pas être reçues car la licence a expiré.

Résoudre l'erreur :

- Achetez une nouvelle licence et activez le produit via le **Gestionnaire de Licences**.

Si vous êtes sûr que la licence n'a pas expiré, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *L'opération réseau a expiré.*

Code d'erreur : `x97`

Description : **L'Updater** Ne peut pas recevoir les mises à jour parce que la connexion a été perdue.

Résoudre l'erreur :

- Vérifiez que la connexion réseau est établie et vérifiez la connectivité. Assurez-vous que votre ordinateur est connecté à Internet.
- Si un serveur proxy est utilisé, vérifiez et configurez les paramètres de connexion.
- Si l'erreur persiste, changez de serveur proxy ou n'utilisez pas de proxy pour les connexions.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Somme de contrôle incorrecte.*

Code d'erreur : `x98`

Description : Un fichier avec des mises à jour reçu par **l'Updater** possède une somme de contrôle qui ne correspond pas à celle attendue.

Résoudre l'erreur :

- Relancez la mise à jour après une durée déterminée.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Fichier clé de démo invalide.*

Code d'erreur : `x99`

Description : Les mises à jour ne peuvent pas être reçues si l'intégrité du fichier clé de démo est violée ou si son utilisation n'est pas autorisée.

Résoudre l'erreur :

- Achetez une licence et activez le produit via le **Gestionnaire de Licences**.

Si vous êtes sûr que le fichier clé de démo est valide, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Clé de licence bloquée.*

Code d'erreur : `x100`

Description : Les mises à jour ne peuvent pas être reçues car l'utilisation du fichier clé est bloquée par **Doctor Web**.



Résoudre l'erreur :

- Achetez une licence et activez le produit via le **Gestionnaire de Licences**.

Si vous êtes sûr que le fichier clé utilisé est valide, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Configuration incorrecte.*

Code d'erreur : `x102`

Description : Un des composants de **Dr.Web pour Linux** ne peut pas fonctionner à cause de paramètres de configuration incorrects.

Résoudre l'erreur :

SpIDer Guard : le mode opératoire indiqué n'est pas supporté par le système d'exploitation.

- Exécutez la commande

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

  Pour passer **SpIDer Guard** en mode automatique.

- Si l'erreur persiste, créez manuellement et installez le module noyau chargeable devant être utilisé par by **SpIDer Guard**.



Notez que le fonctionnement de **SpIDer Guard** et du module noyau chargeable sont garantis uniquement sur les versions testées des **Linux** (voir Pré-requis Système).

Autres composants :

- Restaurer les paramètres par défaut du logiciel. Pour cela
  - Effacez les contenus du fichier `/etc/opt/drweb.com/drweb.ini`. Il est recommandé de faire une copie de sauvegarde du fichier avant la procédure. Par exemple :

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

  - Exécutez la commande

```
# service drweb-configd restart
```

  Pour redémarrer **Dr.Web pour Linux**.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Fichier exécutable invalide.*

Code d'erreur : `x104`

Description : Le fichier exécutable d'un des composants de **Dr.Web pour Linux** est invalide ou corrompu.

Résoudre l'erreur :

- Installez le package avec le composant en question :
  - `drweb-spider`, si le fichier exécutable de **SpIDer Guard** est invalide
  - `drweb-gated`, si le fichier exécutable de **SpIDer Gate**est invalide
  - `drweb-update`, si le fichier exécutable de **l'Updater** est invalide



* Si l'erreur persiste, ou que vous ne pouvez pas voir quel fichier exécutable est invalide, supprimez **Dr.Web pour Linux** et réinstallez-le.
* Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Fichier du noyau moteur invalide.*

Code d'erreur : `x105`

Description : **Dr.Web pour Linux** ne peut pas fonctionner parce que le fichier exécutable du moteur antivirus **Dr.Web Virus-Finding Engine** est invalide ou corrompu.

Résoudre l'erreur :

* Mise à jour des bases virales.
* Si l'erreur persiste, installez le package `drweb-bases` contenant les bases virales et le fichier exécutable du moteur antivirus.
* Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
* Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Pas de base de données virale.*

Code d'erreur : `x106`

Description : **Dr.Web pour Linux** ne peut pas protéger votre ordinateur parce que les bases de données virales sont invalides ou corrompues.

Résoudre l'erreur :

* Mise à jour des bases virales.
* Si l'erreur persiste, installez le package `drweb-bases` contenant les bases virales et le fichier exécutable du moteur antivirus.
* Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
* Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Logiciel incompatible détecté.*

Code d'erreur : `x109`

Description : Un des composants de **Dr.Web pour Linux**peut ne pas fonctionner car un logiciel incompatible a été détecté.

Résoudre l'erreur :

SpIDer Gate : le logiciel détecté qui génère des règles pour le firewall système est incompatible avec le fonctionnement de **SpIDer Gate**.

* Désactivez ou reconfigurez le logiciel afin d'éviter une interférence avec **SpIDer Gate**.

- Sur l'OS **SUSE Linux** avec les paramètres par défaut, des conflits entre **SpIDer Gate** et le firewall système **SuseFirewall2** peuvent survenir. Pour supprimer le conflit, modifiez les paramètres du firewall système **SuseFirewall2**. Pour cela:

  1. Ouvrez le fichier de configuration de **SuseFirewall2** (par défaut, c'est le fichier `/etc/sysconfig/SuSEfirewall2`).
  2. Trouvez le bloc de texte suivant :

```
## Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

  3. Configurez la valeur du paramètre sur `"no"` :

```
FW_LO_NOTRACK="no"
```

  4. Redémarrez **SuseFirewall2**. Pour cela, utilisez la commande suivante :

```
# rcSuSEfirewall2 restart
```



Notez que si le pare-feu n'a pas du paramètre `FW_LO_NOTRACK` dans les paramètres **SuseFirewall2**, il est nécessaire de désactiver le pare-feu pour résoudre le conflit (par exemple, il faut le faire dans l'OS **SUSE Linux Enterprise Server** 11).

  5. Redémarrez **SpIDer Gate** (désactivez-le puis activez-le sur la page correspondante).

Autres composants :

- Désactivez ou reconfigurez le logiciel afin de prévenir une perturbation du fonctionnement de **Dr.Web pour Linux**.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Le composant ScanEngine n'est pas disponible.*

Code d'erreur : `x119`

Description : Impossible de vérifier les fichiers car le module **`drweb-se`** est manquant ou a échoué à démarrer. Ce module est utilisé pour la recherché d'objets malveillants.

Echec au démarrage : **Scanner**, **SpIDer Guard**, **SpIDer Gate** (partiellement).

Résoudre l'erreur :

- Si vous utilisez un OS en version 64-bits, assurez-vous que les bibliothèques de support des applications 32-bits sont installées (voir Pré-requis Système) et, si nécessaire, installez-les. Après l'installation de la bibliothèque de support des applications 32-bits veuillez redémarrer **Dr.Web pour Linux**, en exécutant la commande

```
# service drweb-configd restart
```

- Si votre système d'exploitation utilise **SELinux**, configurez la politique de sécurité pour le module **`drweb-se`** (voir Configurer les Politiques SELinux).
- Exécutez la commande




```
# drweb-ctl cfshow ScanEngine.ExePath
```

Si la chaîne de sortie diffère de `ScanEngine.ExePath = /opt/drweb.com/bin/drweb-se`, exécutez la commande suivante :

```
# drweb-ctl cfset ScanEngine.ExePath /opt/drweb.com/bin/drweb-se
```

- Si l'erreur persiste, installez le composant `drweb-se` (package) séparément.
- Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
- Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Le FileCheck composant n'est pas disponible.*

Code d'erreur : `x120`

Description : Impossible de vérifier les fichiers car le composant du **Scanner** **`drweb-filecheck`** utilisé pour cette fonction, est manquant.

Echec au démarrage : **Scanner**, **SpIDer Guard**.

Résoudre l'erreur :

- Si vous utilisez un OS en version 64-bits, assurez-vous que les bibliothèques de support des applications 32-bits sont installées (voir Pré-requis Système) et, si nécessaire, installez-les.
- Si votre système d'exploitation utilise **SELinux**, configurez la politique de sécurité pour le module **`drweb-filecheck`** (voir Configurer les Politiques SELinux).
- Exécutez la commande

```
# drweb-ctl cfshow FileCheck.ExePath
```

Si la chaîne de sortie diffère de `FileCheck.ExePath = /opt/drweb.com/bin/drweb-filecheck`, exécutez la commande suivante :

```
# drweb-ctl cfset FileCheck.ExePath /opt/drweb.com/bin/drweb-filecheck
```

- Si l'erreur persiste, installez le composant `drweb-filecheck` (package) séparément.
- Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
- Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Le Firewall composant n'est pas disponible.*

Code d'erreur : `x122`

Description : Impossible de contrôler l'accès Internet car **`drweb-firewall`** est manquant ou a échoué à démarrer. Le module est utilisé pour le détournement des connexions.

Echec au démarrage : **SpIDer Gate**.

Résoudre l'erreur :

- Exécutez la commande

```
# drweb-ctl cfshow Firewall.ExePath
```



Si la chaîne de sortie diffère de `Firewall.ExePath = /opt/drweb.com/bin/drweb-firewall`, exécutez la commande suivante :

```
# drweb-ctl cfset Firewall.ExePath /opt/drweb.com/bin/drweb-firewall
```

- Si l'erreur persiste, installez le composant `drweb-firewall` (package) séparément.
- Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
- Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur : *Le NetCheck composant n'est pas disponible.*

Code d'erreur : `x123`

Description : Impossible de contrôler l'accès Internet car **`drweb-netcheck`** est manquant ou a échoué à démarrer. Le module est utilisé pour la vérification des fichiers téléchargés.

Echec au démarrage : **SpIDer Gate** (partiellement).

Résoudre l'erreur :

- Exécutez la commande

```
# drweb-ctl cfshow NetCheck.ExePath
```

Si la chaîne de sortie diffère de `NetCheck.ExePath = /opt/drweb.com/bin/drweb-netcheck`, exécutez la commande suivante :

```
# drweb-ctl cfset NetCheck.ExePath /opt/drweb.com/bin/drweb-netcheck
```

- Si l'erreur persiste, installez le composant `drweb-netcheck` (package) séparément.
- Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
- Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Erreurs sans codes d'erreur

Symptômes :

La fenêtre principale de **Dr.Web pour Linux** est désactivée et affiche le message *Dr.Web pour Linux est en cours de chargement...* ou bien l'indicateur d'état dans la zone de notifications indique une erreur critique, et le menu déroulant contient un seul thème désactivé, **Chargement...**.

Description :

Dr.Web pour Linux ne peut pas démarrer car le composant du noyau **`drweb-configd`** n'est pas disponible.

Résoudre l'erreur :

- Exécutez la commande

```
# service drweb-configd restart
```

Pour redémarrer **Dr.Web pour Linux**.

- Si cette commande remonte un message d'erreur, ou n'a pas d'effet, installez le composant `drweb-configd` (package) séparément.



- Si l'erreur continue à survenir, supprimez **Dr.Web pour Linux** puis installez-le de nouveau.
- Pour en savoir plus sur l'installation et la suppression du produit ou des composants du produit, consultez les manuels utilisateur Procédure d'Installation et Supprimer Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique.

Symptômes :

- L'Indicateur dans la zone de notification du bureau ne s'affiche pas après la connexion au système ;
- La tentative d'exécuter la commande du lancement de l'interface graphique

  ```
  $ drweb-gui
  ```

  ouvre la fenêtre principale de **Dr.Web pour Linux**.

Description :

Cette erreur est liée à l'absence de bibliothèques supplémentaires sur votre **libappindicator1** du système.

Résoudre l'erreur :

- Installez la bibliothèque (le package) **libappindicator1** ; utiliser le gestionnaire de paquets du système.
- Fermer la session et reprendre l'authentification (log in).

Si l'erreur persiste, contactez le Support technique.

Annexe E. Créer un Module Noyau pour SpIDer Guard

Si le système d'exploitation ne supporte pas l'interface de gestion **fanotify**, **SpIDer Guard** utilise un module chargeable spécial fonctionnant dans l'espace noyau.

Par défaut, **SpIDer Guard**est fourni avec un module noyau chargeable complètement intégré pour les OS **CentOS** et **Red Hat Enterprise Linux** en versions 5.10 et 6.5, vu que ces systèmes ne supportent pas **fanotify**. De plus, vous pouvez construire un module noyau chargeable manuellement en utilisant les codes source fournis dans une archive `tar.bz2`.



Le module noyau chargeable utilisé par **SpIDer Guard** est conçu pour fonctionner avec les noyaux **Linux** 2.6 et supérieurs.

L'archive contenant les codes source est situé dans le sous-répertoire `share/drweb-spider-kmod/src` du répertoire de base de **Dr.Web pour Linux** (par défaut `/opt/drweb.com`). Le nom de l'archive est construit comme suit : **drweb-spider-kmod-<version>-<date>.tar.bz2**.

Le répertoire `drweb-spider-kmod` contient également le script de test **check-kmod-install.sh**. Exécutez le script pour vérifier si l'OS utilisé supporte les versions du module noyau inclus au produit. Si ce n'est pas le cas, un message vous invitant à créer manuellement le module s'affiche sur l'écran.



Pour créer le module noyau chargeable manuellement d'après les codes source, les privilèges administrateur (root) sont requis. Pour cela, vous pouvez utiliser la commande **su** pour passer à un autre utilisateur ou la commande **sudo** pour créer le module en tant qu'autre utilisateur.

Pour créer le module noyau

1. Décompressez l'archive contenant les codes source dans n'importe quel dossier. Par exemple, la commande

```
# tar -xf drweb-spider-kmod-<version>-<date>.tar.bz2
```

décompresse les codes source dans le dossier créé. Ce dossier comporte le nom de l'archive et est créé au même endroit que celui où réside l'archive.

2. Allez au dossier créé et exécutez la commande suivante :

```
# make
```

Si une erreur survient durant **l'exécution de la commande make**, réparez-la (voir ci-dessous) et relancez la compilation.

3. Une fois la commande exécutée avec succès, entrez les commandes suivantes :

```
# make install
# depmod
```

4. Une fois le module noyau compilé avec succès et enregistré dans le système, effectuez les paramétrages supplémentaires de **SpIDer Guard**. Paramétrez le composant afin qu'il fonctionne avec le module noyau en exécutant la commande suivante :

```
# drweb-ctl cfset LinuxSpider.Mode LKM
```

Vous pouvez également indiquer `AUTO` au lieu de `LKM`. Dans le dernier cas, **SpIDer Guard** tentera d'utiliser le module noyau et l'interface de gestion **fanotify**. Pour en savoir plus, utilisez la commande suivante :

```
$ man drweb-spider
```



Erreurs de création possibles

Durant l'exécution de la commande **make**, des erreurs peuvent survenir. Si c'est le cas, vérifiez les éléments suivants :

- Pour garantir une création réussie du module, **Perl** et **GCC** sont requis. S'ils ne sont pas présents dans le système, installez-les.
- Sur certains OS, vous pouvez avoir besoin d'installer le package **kernel-devel** avant de lancer la procédure.
- Sur certains OS, la procédure peut échouer parce que le chemin vers le répertoire contenant les codes source a été indiqué de manière incorrecte. Si c'est le cas, indiquez la commande **make** avec le paramètre `KDIR=/path/to/kernel/source/codes`. Typiquement, les codes source sont situés dans le répertoire `/usr/src/kernels/<kernel_version>`. Notez que la version du noyau remontée par la commande **uname** `-r` peut différer du nom de répertoire `<kernel_version>` !